

nLite Wireless 3G Broadband Router

3G-6200n

User Manual

Version 1.0 / 3, 2009





Copyright© by Edimax Technology Co, LTD. all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical , chemical, manual or otherwise, without the prior written permission of this company.

This company makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

Notice according to GNU/GPL-Version 2

This product includes software that is subject to the GNU/GPL-Version 2. You find the text of the license on the product cd/dvd. The program is free software and distributed without any warranty of the author. We offer, valid for at least three years, to give you, for a charge no more than the costs of physically performing source distribution, a complete machine-readable copy of the corresponding source code. Please contact Edimax at: Edimax Technology co., Ltd, NO. 3, Wu-Chuan 3rd RD Wu-Ku-Industrial Park, Taipei Hsien, Taiwan. R.O.C., TEL : +886-2-77396888, FAX : +886-2-77396887, sales@edimax.com.tw

- ※ The product you have purchased and the setup screen may appear slightly different from those shown in this QIG. For more detailed information about this product, please refer to the User's Manual on the CD-ROM.
- ※ Software and specifications subject to change without notice. Please visit our web site for the update.
- ※ All rights reserved. Trademarks or registered trademarks are the property of their respective holders

| | |
|--|----|
| Introduction | 4 |
| Chapter 1 | 18 |
| 1.1 Cable Modem..... | 30 |
| 1.2 Fixed-IP xDSL..... | 31 |
| 1.3 PPPoE | 32 |
| 1.4 PPTP | 34 |
| 1.5 L2TP | 36 |
| 1.6 Telstra Big Pond..... | 38 |
| Chapter 2 | 40 |
| 2.1 System..... | 42 |
| 2.1.1 Time Zone | 43 |
| 2.1.2 Password Settings | 43 |
| 2.1.3 Remote Management | 45 |
| 2.2 3G/3.5G | 47 |
| (A) Plug and play, no setup procedure required. | 47 |
| (B) PIN code or user name / password required:..... | 48 |
| 2.3 WAN..... | 48 |
| 2.3.1 Dynamic IP..... | 49 |
| 2.3.2 Static IP Address | 50 |
| 2.3.3 PPPoE (PPP over Ethernet) | 50 |
| 2.3.4 PPTP | 50 |
| 2.3.5 L2TP | 50 |
| 2.3.6 Telstra Big Pond..... | 50 |
| 2.3.7 DNS | 51 |
| 2.3.8 DDNS..... | 51 |
| 2.4 LAN..... | 53 |
| 2.5 Wireless | 55 |
| 2.5.1 Basic Settings | 56 |
| 2.5.2 Advanced Settings | 58 |
| 2.5.3 Security | 60 |
| 2.5.3.1 WEP only | 60 |
| 2.5.3.2 802.1x only..... | 62 |
| 2.5.3.3 802.1x WEP Static key..... | 63 |
| 2.5.3.4 WPA Pre-shared key | 64 |

| | |
|------------------------------------|-----|
| 2.5.3.5 WPA Radius | 65 |
| 2.5.4 Access Control | 65 |
| 2.6 QoS..... | 69 |
| 2.7 NAT | 72 |
| 2.7.1 Port Forwarding | 74 |
| 2.7.2 Virtual Server | 76 |
| 2.7.3 Special Applications | 78 |
| 2.7.4 UPnP Settings..... | 81 |
| 2.7.5 ALG Settings..... | 82 |
| 2.7.6 Static Routing..... | 83 |
| 2.8 Firewall..... | 85 |
| 2.8.1 Access Control | 86 |
| 2.8.2 URL Blocking | 86 |
| 2.8.3 DoS (Denial of Service)..... | 93 |
| 2.8.4 DMZ | 94 |
| Chapter 3 | 95 |
| 3.1 Status and Information | 96 |
| 3.2 Device Status | 98 |
| 3.3 System Log | 99 |
| 3.4 Security Log | 100 |
| 3.5 Active DHCP Client | 101 |
| 3.6 Statistics..... | 102 |
| Chapter 4 | 103 |
| 4.1 Configuration Tools | 103 |
| 4.2 Firmware Upgrade | 104 |
| 4.3 Reset | 105 |
| Appendix A..... | 107 |
| Glossary..... | 109 |

Introduction

Thank you for purchasing Edimax 3G-6200n nLite wireless 3G broadband router! This high cost-efficiency router is the best choice for Mobile / Small office / Home office users, all computers and network devices can share a single wireless 3G modem or xDSL / cable** modem internet connection at high speed. Easy install procedures allows any computer users to setup a network environment in very short time - within minutes, even inexperienced. When the number of your computers and network-enabled devices grow, you can also expand the number of network slot by simple attach a hub or switch, to extend the scope of your network!

You can configure the router by running the Setup Wizard in the CD-ROM provided in the package. The wizard provides quick setup for wireless 3G/3.5G Internet connection, Ethernet WAN Internet connection, SSID, wireless security, firmware upgrade and changing router's password. When you start the Setup Wizard, you will get the following Welcome screen. Please choose the language to start with and follow the easy steps in the Wizard. No instruction for the Setup Wizard is given here.

If you lost the CD-ROM or you prefer the traditional web setup, please follow the procedures in Manual to configure the router.



Note 1: Only one Internet connection (wireless 3G or xDSL/Cable) can be used at the same time.

Note 2: To prevent the compatibility problem between 3G USB Modem and 3G router, it is recommended that you upgrade the latest firmware of 3G router from Edimax website <http://www.edimax.com> .

Features

- Provides IEEE 802.11g/b wireless LAN access point
- Compatible with IEEE 802.11n standard with 150Mbps data rate
- High Internet access throughput
- Allow multiple users to share a single Internet connection
- Supports up to 253 network client users
- Provides one USB port for 3G wireless connection
- Internet Access via 3G modem or Cable or xDSL modem
- Access Servers on your LAN from the Public Network
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M)
- Support DHCP (Server/Client) for easy setup
- Support advance features such as: special applications, DMZ, virtual server, access control, firewall
- Allow you to monitor the router's status such as: DHCP Client Log, System Log, Security Log and Device/Connection Status
- Easy to use Web-based GUI for configuration and management
- Remote Management allows configuration and upgrades from a remote site (over the Internet)

Minimum Requirements

- One External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45)
- Network Interface Card (NIC) for each Personal Computer (PC)
- Computer with a Web-Browser (Internet Explorer 5.0 or higher / Netscape Navigator 7.2 or higher)

Package Contents

- One Wireless 3G broadband router
- One Quick Installation Guide
- One CD-ROM (Wizard, Multi-languages QIG and User Manual)
- One Power Adapter
- Ethernet Cable
- Holding base
- Accessories

Note

The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software

sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by access time.

Back Panel

The diagram (fig1.0) below shows the broadband router's back panel. The router's back panel is divided into four sections, LAN, WAN, USB, and Reset:

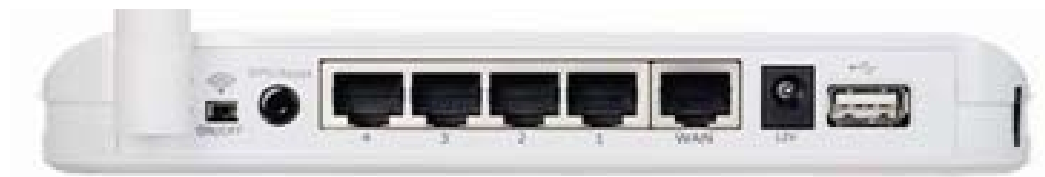


Figure 1.0

1) Local Area Network (LAN)

The Broadband router's 4 LAN ports are where you connect your LAN's PCs, hubs / switches etc.

2) Wide Area Network (WAN)

The WAN port connected to your xDSL or Cable modem which linked to the Internet.

3) USB

The USB port allow you to share internet via 3G USB modem card.

4) WPS / Reset button

You can press the button 2~4 seconds to enable WPS for wireless security.

When you experience some problem on using this router, or you forgot your password, you can press the reset button for **longer** than 20 seconds and the router will reset itself to the factory default settings (**warning**: your original configurations will be replaced with the factory default settings)

5) Wireless on/off



You can enable/disable WiFi wireless signal via switch button.

Front Panel

On the router's front panel there are LEDs, which shows the status of this router. Below is the list of each LED and its description.



Figure 1.1

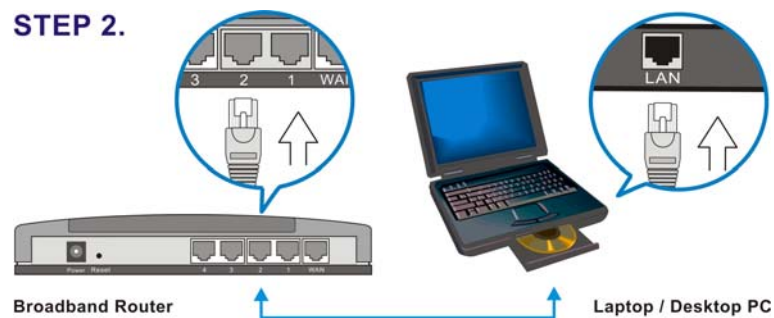
| LED | Light Status | Description |
|---|--------------|---|
|  | ON | Router is powered on |
| WAN LNK/ACT | ON | WAN is connected |
| | Off | WAN is unconnected |
| | Flashing | WAN port is sending / receiving data |
| LAN LNK/ACT (Port 1-4) | ON | LAN port is connected |
| | Off | LAN port is unconnected |
| | Flashing | LAN port is sending / receiving data |
| 3G | ON | 3G USB modem is connected |
| | Off | 3G USB modem is not connected |
| | Flashing | 3G USB modem card is sending / receiving data |
|  | ON | Wireless LAN has been activated |
| | Off | Wireless LAN is disabled |
| | Flashing | Wireless LAN is sending / receiving data |

Setup Diagram

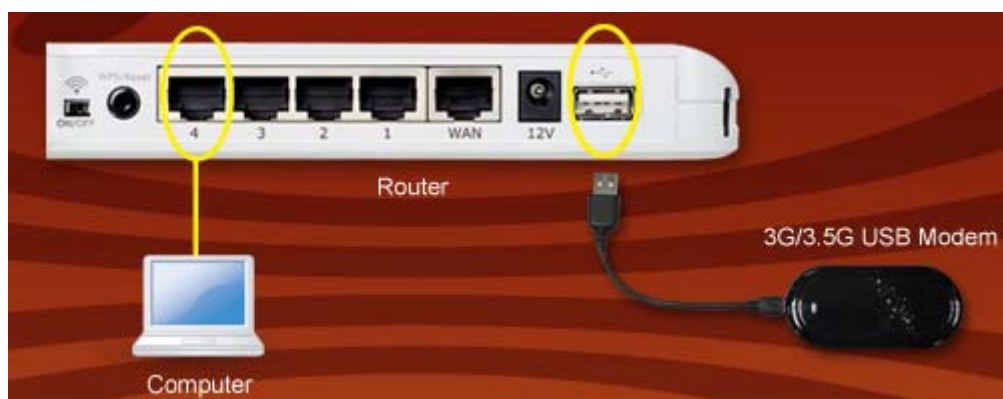
(A) 3G/3.5G Modem card installation:

If you have 3G/3.5G modem card and SIM card, please follow the following instructions to establish connection

1. Connect power adapter to 3G-6200n
2. Connect another Ethernet cable from the any LAN ports (1~4) on router to the Ethernet socket on the PC



3. Insert SIM card into 3G/3.5G modem card, and connect the modem card with one of USB port of 3G-6200n. The corresponding USB LED indicator on 3G-6200n will light.

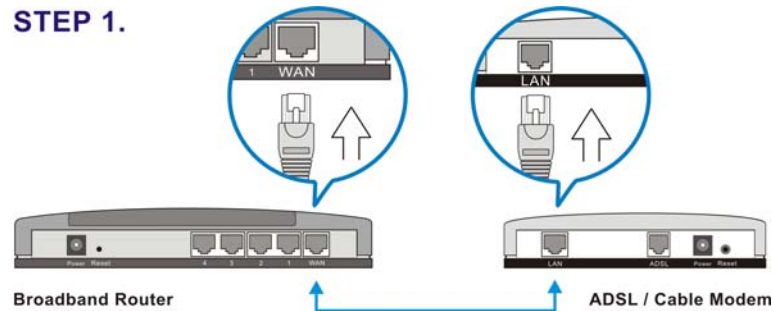


(B) Cabling installation:

If you can also access Internet by xDSL/Cable modem, please follow the following instructions:

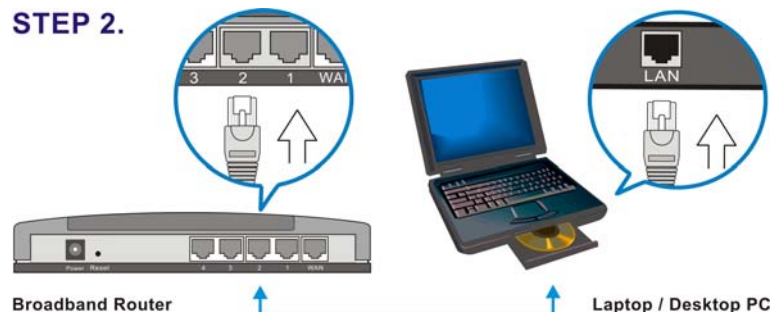
1. Connect the Ethernet cable from the router's WAN port to the LAN port of the modem.

STEP 1.



2. Connect another Ethernet cable from the any LAN ports (1~4) on router to the Ethernet socket on the PC.

STEP 2.



3. Check to make sure the router's LINK LED is lit; to confirm the cable connections are made correctly.

Getting started

This is a step-by-step instruction on how to start using the router and get connected to the Internet.

- 1) Setup your network as shown in the setup diagram above (fig 1.2).
- 2) You will need to set your LAN PC clients so that it can obtain an IP address automatically. All LAN clients require an IP address. Just like the mailing address in real world, it allows LAN clients to find one another. (If you already configured your PC to obtain an IP automatically, please jump to step 3, page 11)

Configure your PC to obtain an IP address automatically

Broadband router's DHCP function is switched on by default; this means that you can obtain an IP address automatically once you've configured your PC to obtain an IP address automatically. This section will show you how to configure your PC's so that it can obtain an IP address automatically for either Windows 95/98/Me, 2000 or NT operating systems. For other operating systems (Macintosh, Sun, etc.), follow the manufacturer's instructions. The following is a step-by-step illustration on how to configure your PC to obtain an IP address automatically for:

- 2a) **Windows 95/98/Me**
- 2b) **Windows XP**
- 2c) **Windows 2000**, and
- 2d) **Windows NT**.

2a) Windows 95/98/Me

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear.
3. Check your list of Network Components. If TCP/IP is not installed, click the *Add* button to install it; if TCP/IP is installed, jump to **step 6**.
4. In the *Network Component Type* dialog box, select *Protocol* and click *Add* button.
5. In the *Select Network Protocol* dialog box, select *Microsoft* and *TCP/IP* and then click the *OK* button to start installing the TCP/IP protocol. You may need your Windows installation CD to complete the installation.
6. After installing TCP/IP, go back to the *Network* dialog box. Select TCP/IP from the list of Network Components and then click the *Properties* button.
7. Check each of the tabs and verify the following settings:

- Gateway:** All fields are blank.
- DNS Configuration:** Select *Disable DNS*.
- WINS Configuration:** Select *Disable WINS Resolution*.
- IP Address:** Select *Obtain IP address automatically*.



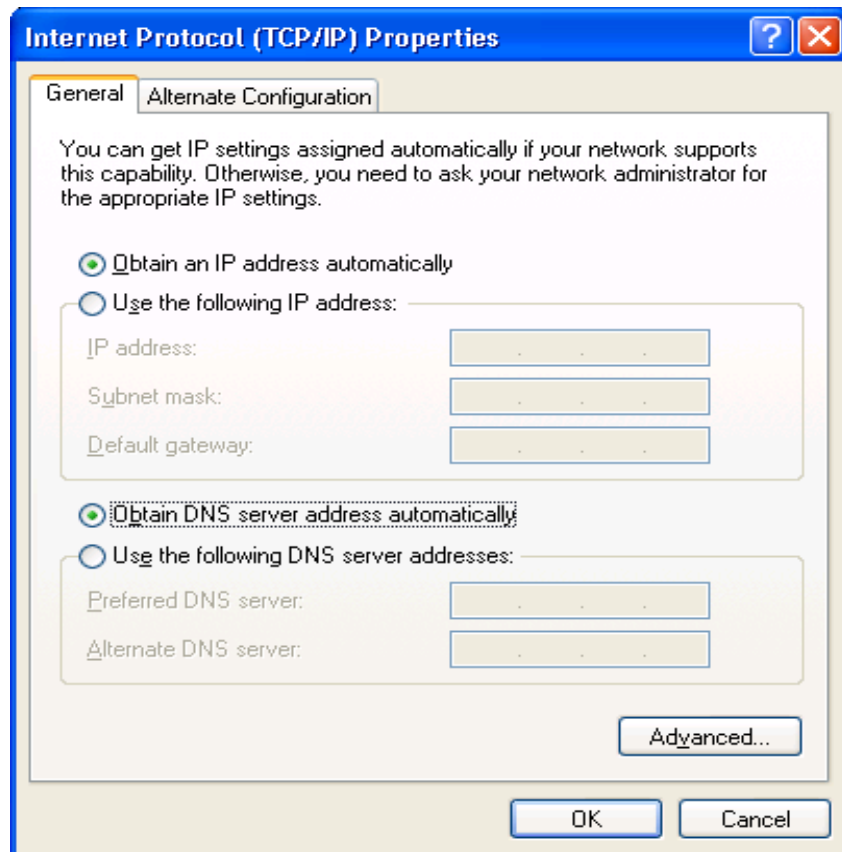
8. Reboot the PC. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

2b) Windows XP

1. Click the *Start* button and select *Settings*, then click *Network Connections*. The *Network Connections* window will appear.
2. Double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
4. In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



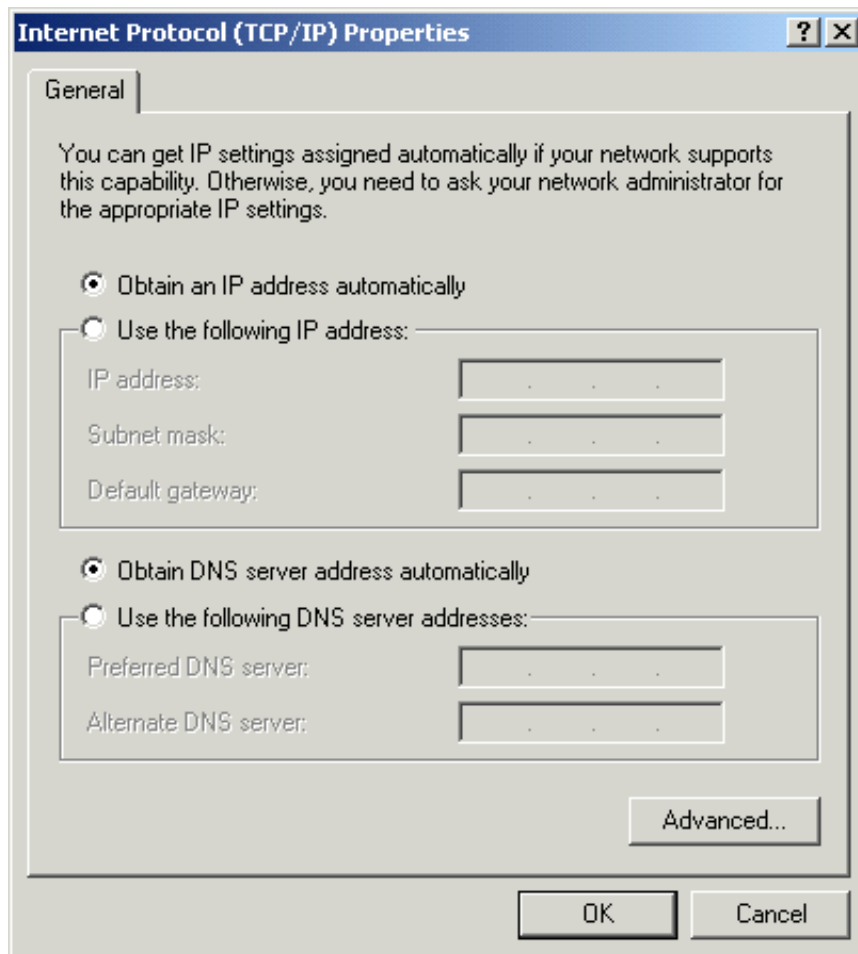
5. Click **OK** to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

2c) Windows 2000

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network and Dial-up Connections* icon. In the *Network and Dial-up Connection* window, double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. In the *Local Area Connection* window, click the *Properties* button.
4. Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
5. In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



6. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

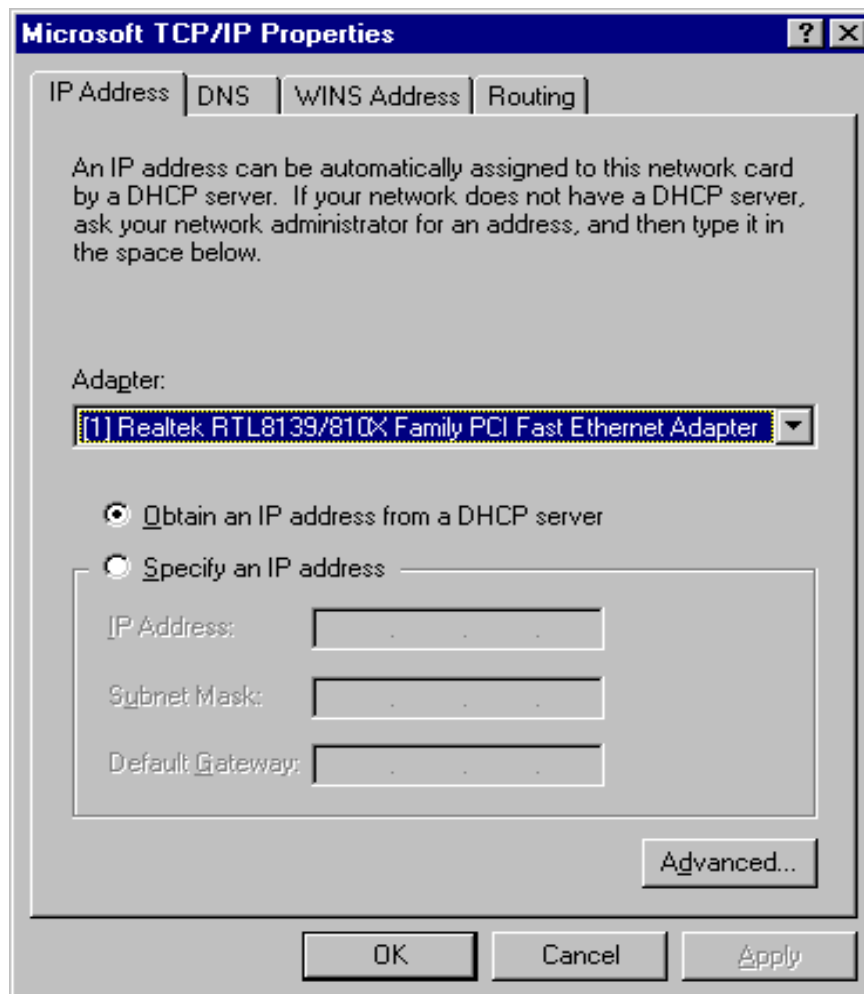
Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

2d) Windows NT

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear. Select the *Protocol* tab from the *Network* window.
3. Check if the *TCP/IP Protocol* is on your list of *Network Protocols*. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to **step 5**.
4. In the *Select Network Protocol* window, select the *TCP/IP Protocol* and click the *Ok* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.

5. After you install TCP/IP, go back to the Network window. Select TCP/IP from the list of Network Protocols and then click the Properties button.
6. Check each of the tabs and verify the following settings:
 - **IP Address:** Select *Obtain an IP address from a DHCP server*.
 - **DNS:** Make all fields blank.
 - **WINS:** Make all fields blank.
 - **Routing:** Make all fields blank.



7. Click **OK** to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router is the only DHCP server on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3

- 3) Once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give each of your LAN clients an IP address. By default the Broadband Router's DHCP server is enabled so that you can obtain an IP address

automatically. To see if you have obtained an IP address, see Appendix A.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server on your LAN. If there is another DHCP on your network, then you'll need to switch one of the DHCP servers off. (To disable the Broadband router's DHCP server see chapter 2 LAN Port)

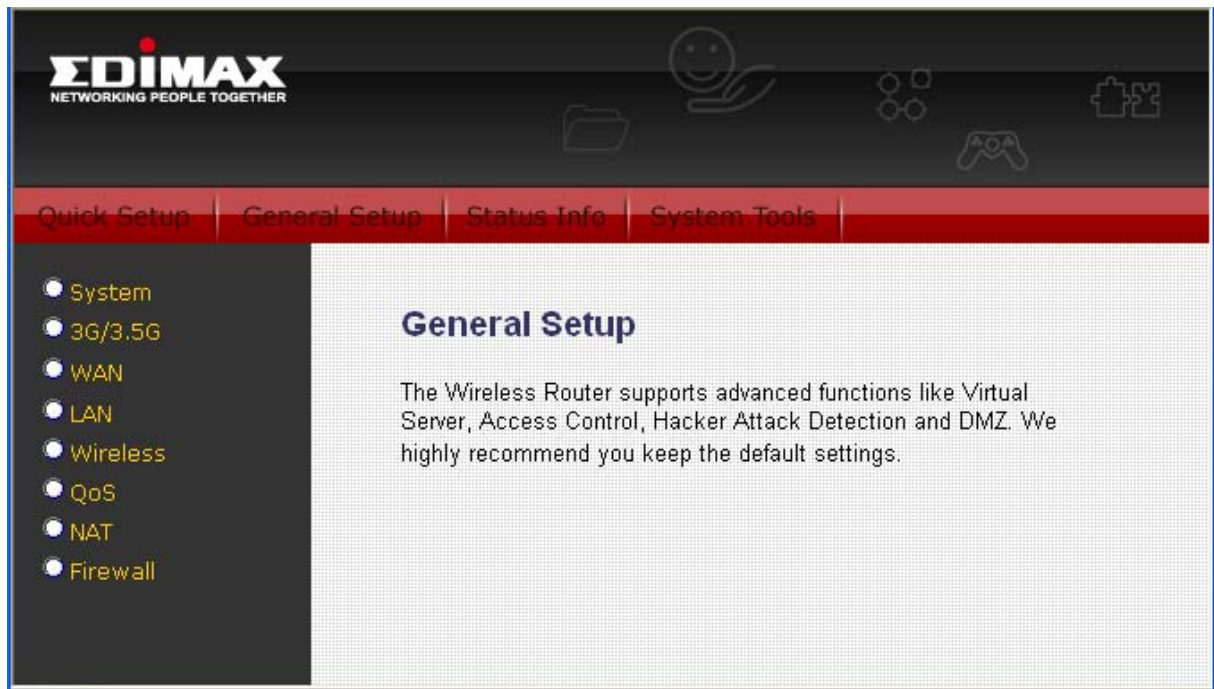
4) Once your PC has obtained an IP address from your router, enter the default IP address **192.168.2.1** (broadband router's IP address) into your PC's web browser and press <enter>

5) The login screen below will appear. Enter the "User Name" and "Password" and then click <OK> to login.

Note: By default the user name is "**admin**" and the password is "**1234**". For security reasons it is recommended that you change the password as soon as possible (in General setup / system / password, see chapter 2)



6) The **HOME** page screen below will appear. The **Home** Page is divided into four sections, **Quick Setup Wizard**, **General Setup**, **Status Info** and **System Tools**.



Quick Setup Wizard (*Chapter 1*)

Select your Internet connection type and setup the configurations needed to connect to your Internet Service Provider (ISP).

General Setup (*Chapter 2*)

This section contains configurations for the Broadband router's advanced functions such as: address mapping, virtual server, access control, hacker attack prevention, DMZ, special applications and other functions to meet your needs.

Status Info (*Chapter 3*)

In this section you can see the Broadband router's system information, Internet Connection, Device Status, System Log, Security Log and DHCP client information.

System Tools (*Chapter 4*)

This section contains the broadband router's tool sets - tools include configuration, firmware upgrade and Reset. Configuration tools allow you to backup (save), restore, or restore to factory default configuration for your Broadband router. The firmware upgrade tool allows you to upgrade your Broadband router's firmware. The RESET tool allows you to reset your Broadband router.

- 7) Click on **Quick Setup Wizard** (see chapter 1) to start configuring settings required by your ISP so that you can start accessing the Internet. The other sections (General Setup, Status Information and

Tools) do not need to be configured unless you wish to implement / monitor more advanced features/information.

Select the section (Quick Setup Wizard, General Setup, Status Information and Tools) you wish to configure and proceed to the corresponding chapter.

Chapter 1

Quick Setup

The Quick Setup section is designed to get you using the broadband router as quickly as possible. In the Quick Setup you are required to fill in only the information necessary to access the Internet. Once you click on the **Quick Setup Wizard** in the HOME page, you should see the screen below.

Step 1) Time Zone

The Time Zone allows your router to base its time on the settings configured here, this will affect functions such as log entries and firewall settings.

EDIMAX
NETWORKING PEOPLE TOGETHER

Quick Setup | General Setup | Status Info | System Tools

1. Time Zone
2. WAN Type
3. IP Address Info

Time Zone ?

Set the time zone of the Wireless Router. This information is used for log entries and firewall settings.

Time Zone : (GMT+00:00)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Time Server Address : 192.43.244.18

Daylight Savings : ☐ Enable
Time From : January 1 To : January 1

NEXT

| Parameter | Description |
|---------------------|---|
| Set Time Zone | Select the time zone of the country you are living. The router will set its time based on your selection |
| Time Server Address | You can manually assign time server address if the default time server dose not work |
| Daylight Savings | The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below) |
| Times From | Select the period in which you wish to start using daylight saving |
| Times to | Select the period in which you wish to stop using daylight saving |

Click on **NEXT** to proceed to the next page (step 2): Broadband Type.

Step 2) 3G/3.5G Internet Configuration

3G-6200n supports most of 3G/3.5G modem cards, just connect the modem card to the USB port of 3G-6200n and 3G-6200n will recognize it automatically, no additional setup procedure required. However, some of modem cards require PIN code or account / password (you have to use 3G-6200n's web interface to input these information), and some modem cards requires you to connect the modem card with your PC and install driver / utility before you connect it with 3G-6200n (all PCs which need to access Internet by 3G-6200n requires to perform this procedure once). If you still not able to connect to Internet, please use wired Internet connection to access our website :<http://www.edimax.com/> ,download latest version of firmware and upgrade 3G-6200n's firmware. If you still not be able to get connected by your 3G/3.5G modem card, please contact your dealer of purchase and provide the model name of the 3G/3.5G modem card you have, we'll try our best to help you to solve the problem.

Only one Internet connection (wireless / wired) can be used at the same time. Wireless connection (3G/3.5G) will be selected first, and use wired Internet connection as backup. Therefore, please DO NOT connect your 3G/3.5G modem card with 3G-6200n, or your telecomm service provider may charge you with high communication fee. For example, if you connect 3G/3.5G modem card with 3G-6200n when you're using wired Internet connection, wired connection will be dropped and use 3G/3.5G wireless connection instead. If 3G/3.5G wireless signal reception is poor and the connection can not be restored within 60 seconds, 3G-6200n will use wired Internet connection again, and will not switch back to wireless Internet connection (This only happens with wired Internet connection is available. If wired connection is unavailable, 3G-6200n will try to establish 3G/3.5G wireless connection again and again). If you want to use 3G/3.5G wireless connection again, you need to remove 3G/3.5G modem card from 3G-6200n and reconnect it back after 5 seconds.

(A) Plug and play, no setup procedure required.

Connect the USB 3G/3.5G modem card with 3G-6200n and make sure the corresponding USB LED indicator of 3G-6200n lights up, then you can use the web browser to access Internet.

(B) PIN code or user name / password required:

Please check the authentication method you want to use. Most of telecomm service providers require you to input PIN Code, please check 'SIM' and input the PIN code provided by telecomm service provider. Most of options listed here are optional and you don't have to provide those information if telecomm service provider doesn't provide you with those information.

If telecomm provider provides you with username / password, please check /User Name / Password box and input the user name / password provided by telecomm service provider, then click 'OK' button. Wait for 1 minute (for 3G-6200n to reboot), then you can access Internet.

Quick Setup | **General Setup** | **Status Info** | **System Tools**

1. Time Zone
2. WAN Type
3. IP Address Info

☒ **3G/3.5G**
If you connect to Internet using an 3G/3.5G handset or 3G/3.5G USB modem, then you should choose this option and enter the required information.

☐ **Cable Modem**
A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Wireless Router will automatically establish a connection, so you probably do not need to enter anything more.

☐ **Fixed-IP xDSL**
Some xDSL Internet Service Providers may assign a Fixed IP Address for your Wireless Router. If you have been

Please input User name & Password in "PPP Settings" and do not input them in "Network Settings" unless your ISP ask you input them in both.

PPP Settings :

Username :

Password :

Idle Timeout :

Echo Timeout :

Echo Count :

Network Settings :

User Name (Optional)

Password (Optional)

Enter PIN Code

APN

Service

Apply Cancel

Note: Please choose "CDMA", if your ISP use 3G CDMA system.

Service

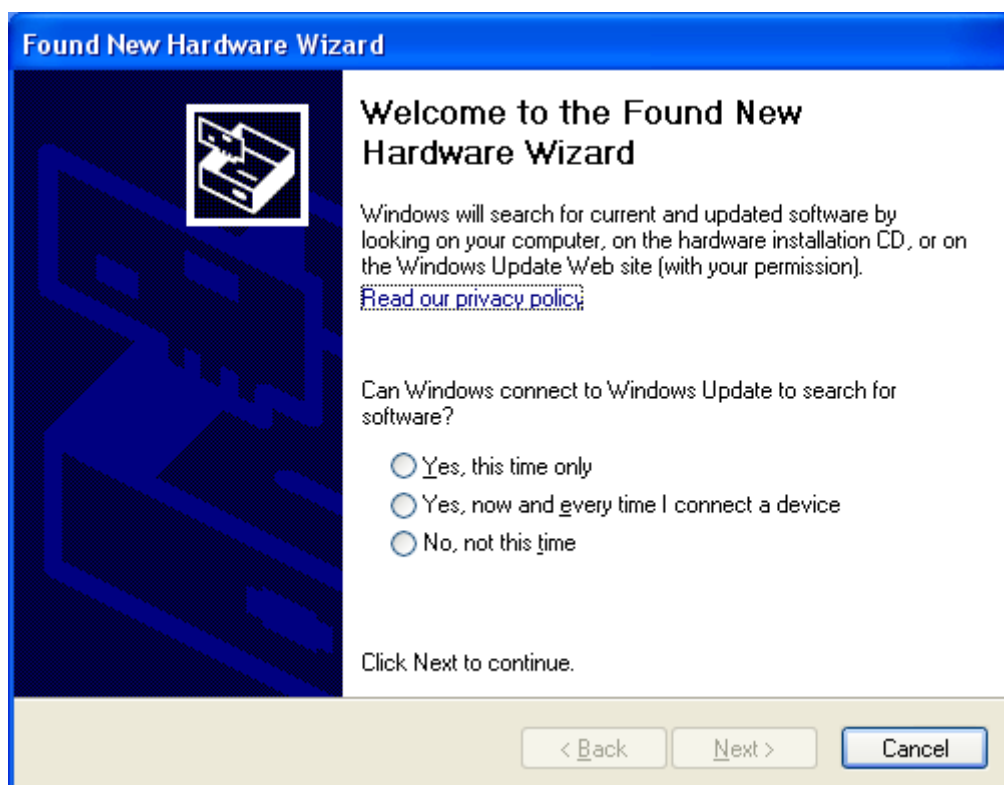
(C) Driver / Utility required on PC side

Some 3G/3.5G modem card does not work with instructions (A) or (B) listed above (ex. BandLuxe C100S). You need to install 3G/3.5G modem card driver / utility on every PC which needs to access Internet first. After driver / utility installation is complete, every PC will be able to access Internet via 3G/6200n.

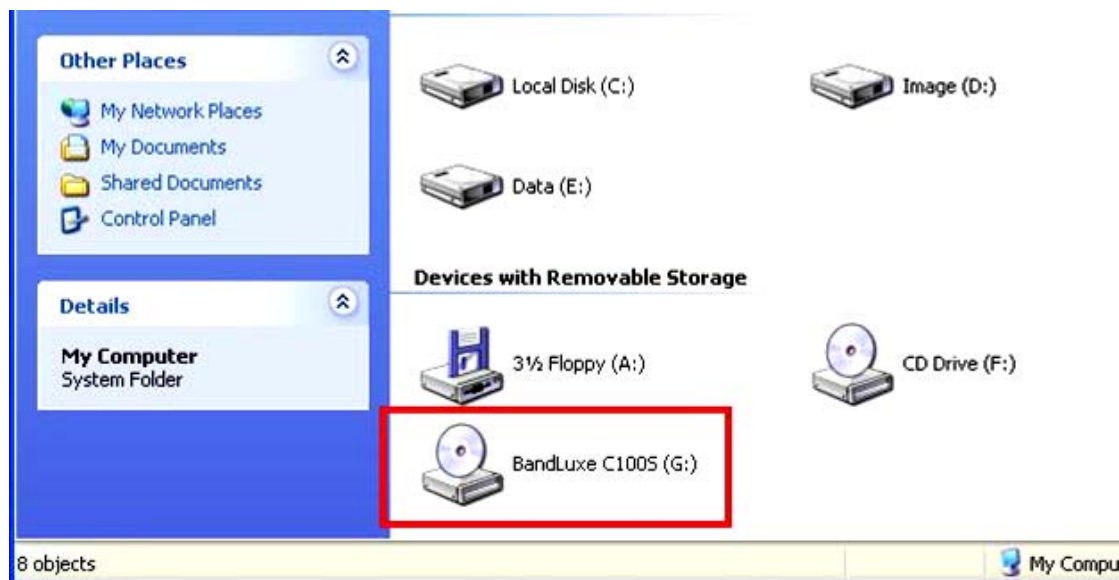
1. Plug in the BandLuxe C100S modem card to the USB port of your computer.
2. The system will detect the hardware of C100S USB adapter and also the storage inside the adapter.



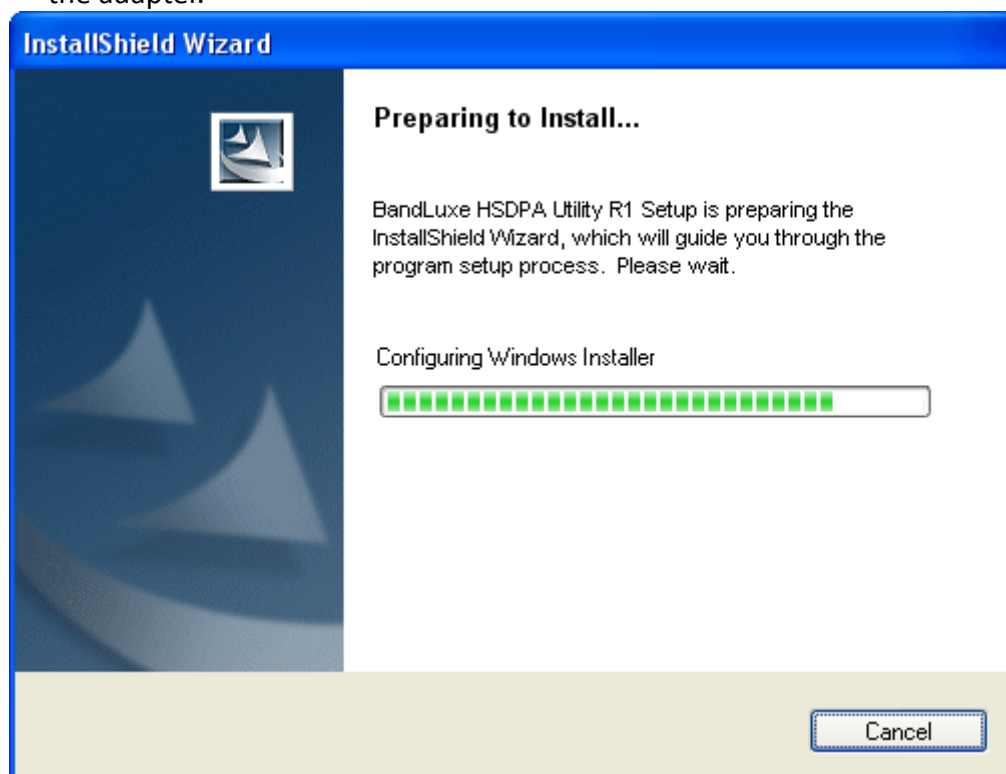
3. Please click "Cancel" to ignore the message of the found new hardware wizard.



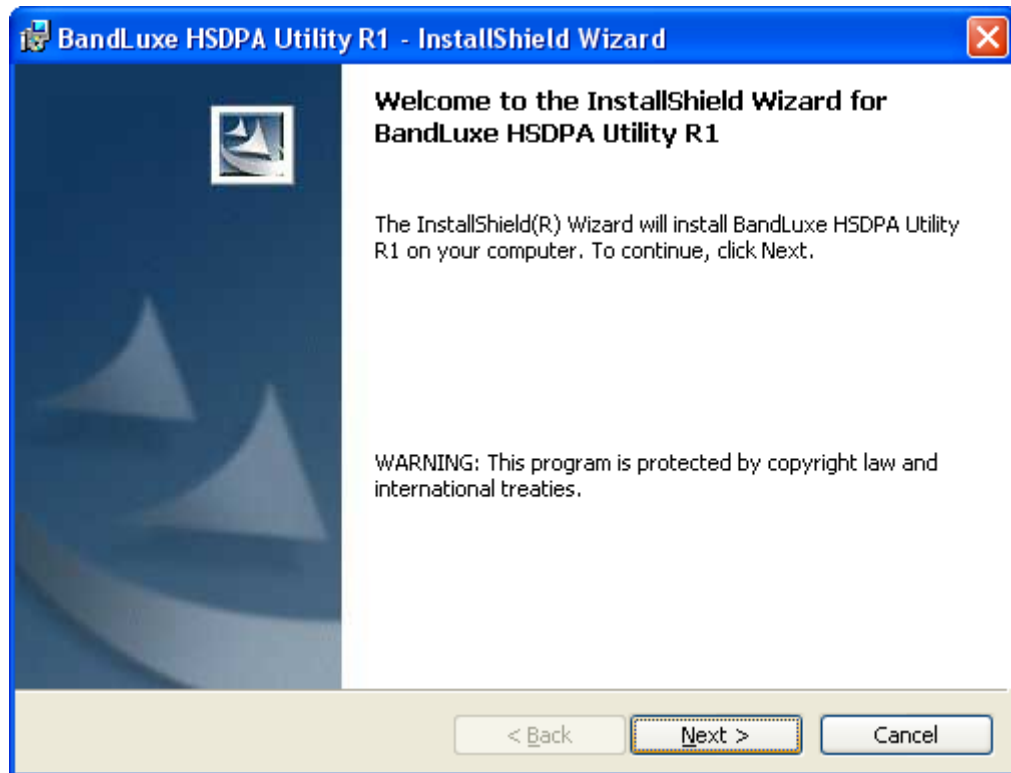
4. Please go to “My computer”, you will see the BandLuxe C100S. Double click the device.



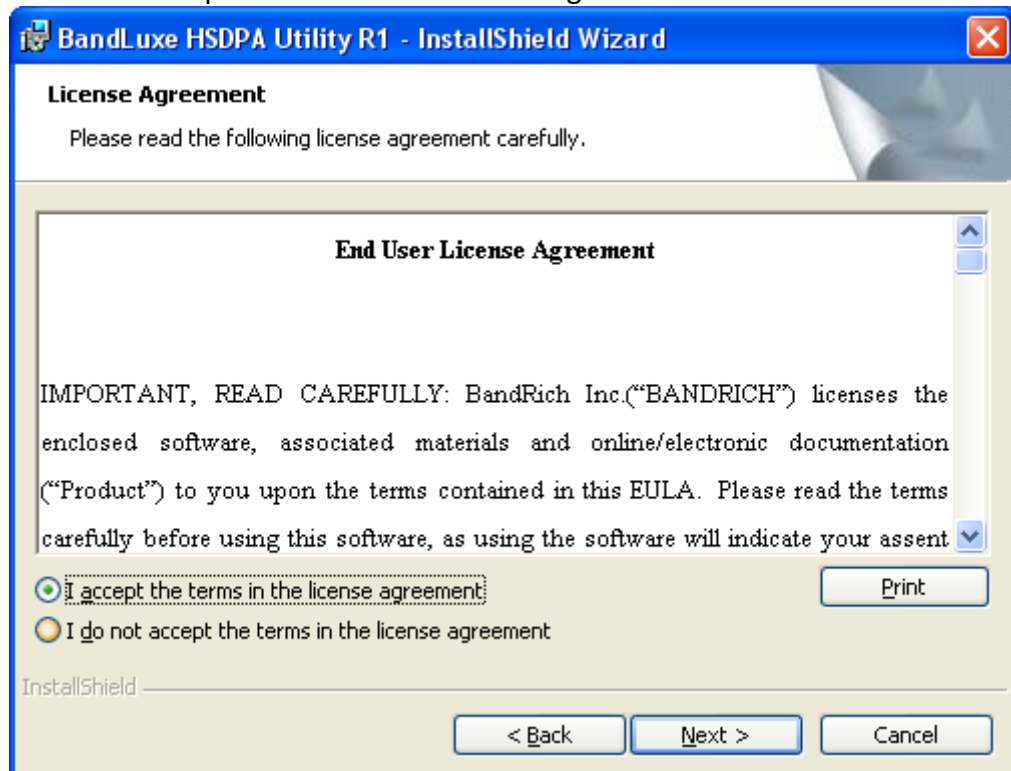
5. The program inside the adapter will prepare to install the driver and utility of the adapter.



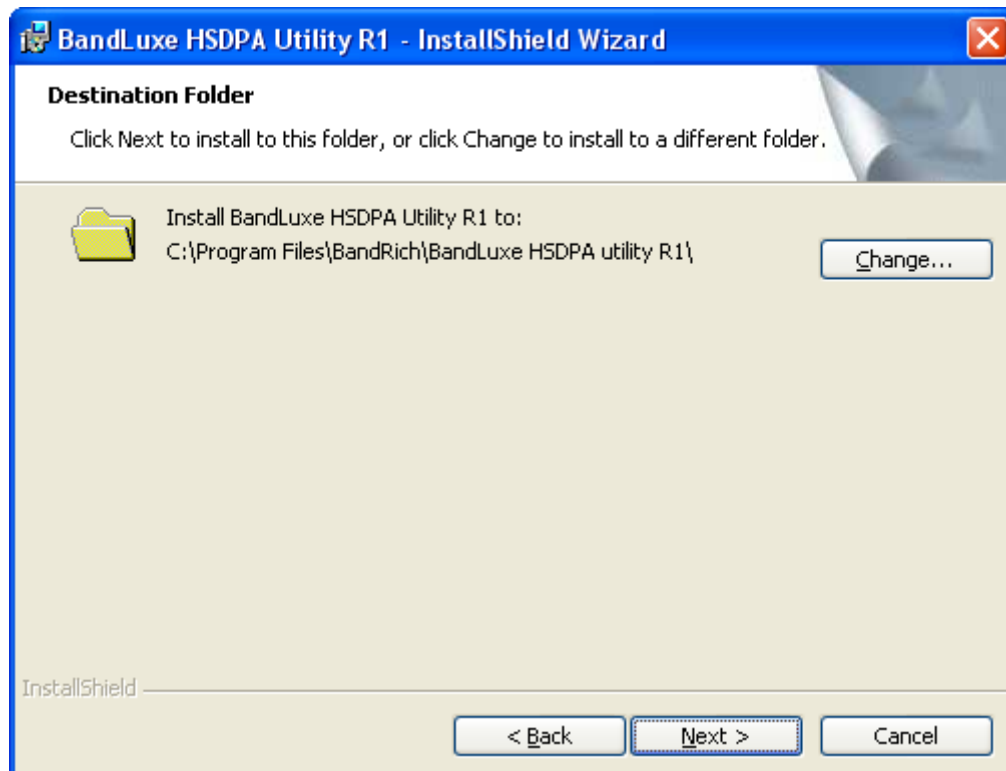
6. Click “Next”.



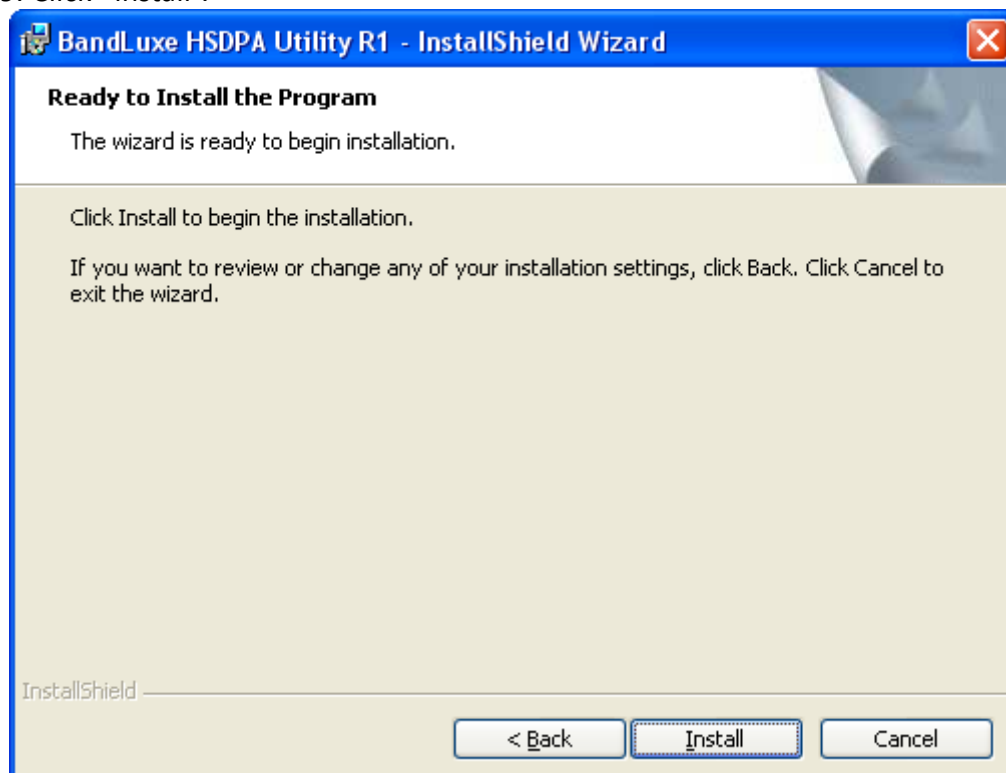
7. Select “I accept the terms in the license agreement” and click “Next”.



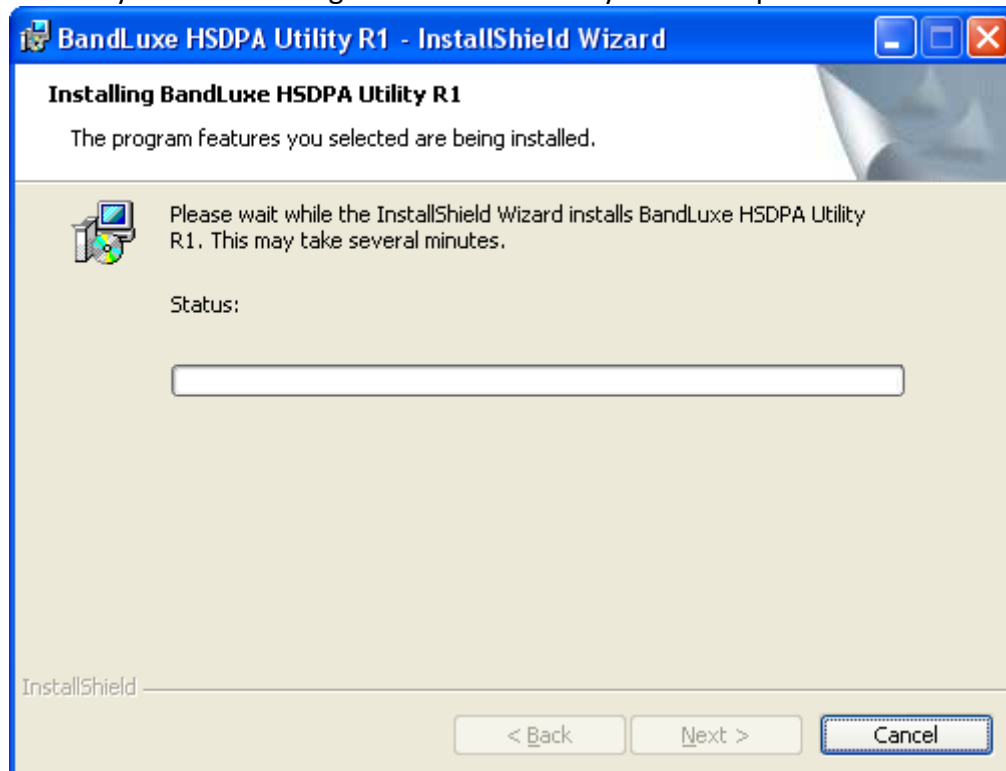
8. If you want to change the destination folder, please click “Change”. Click “Next” to continue.



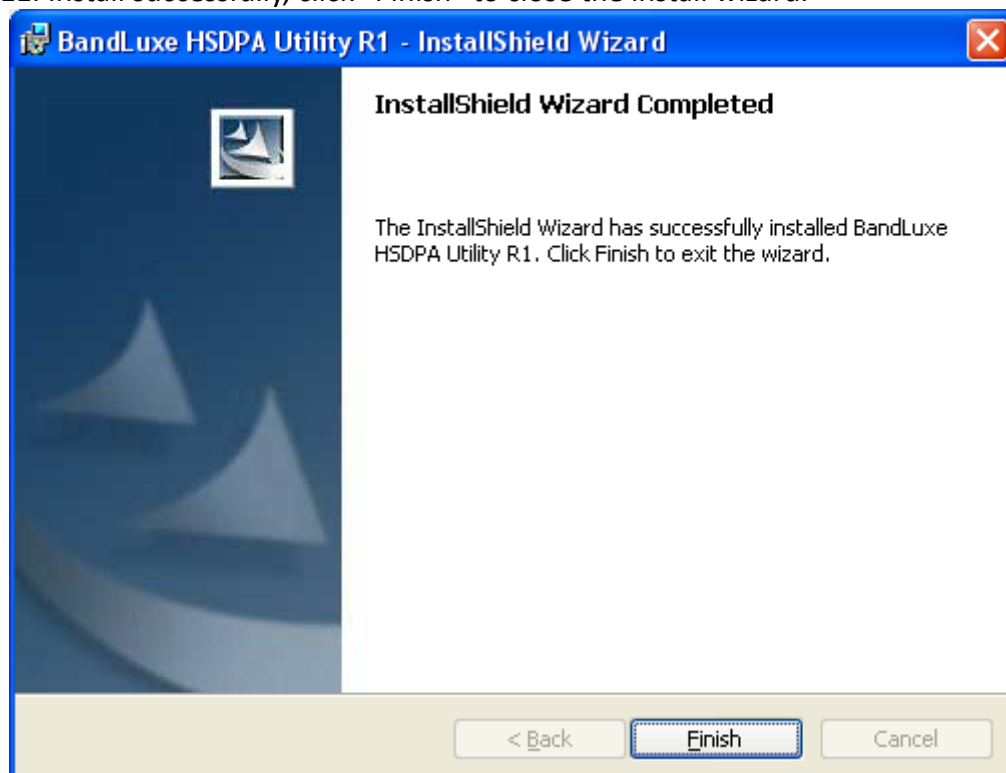
9. Click “install”.



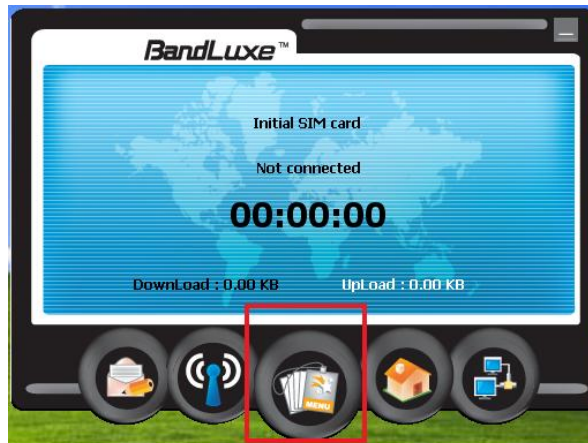
10. The system is installing the driver and utility of the adapter.



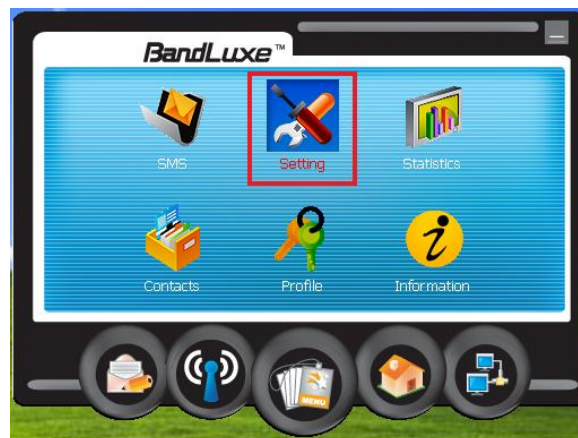
11. Install successfully, click "Finish" to close the install wizard.



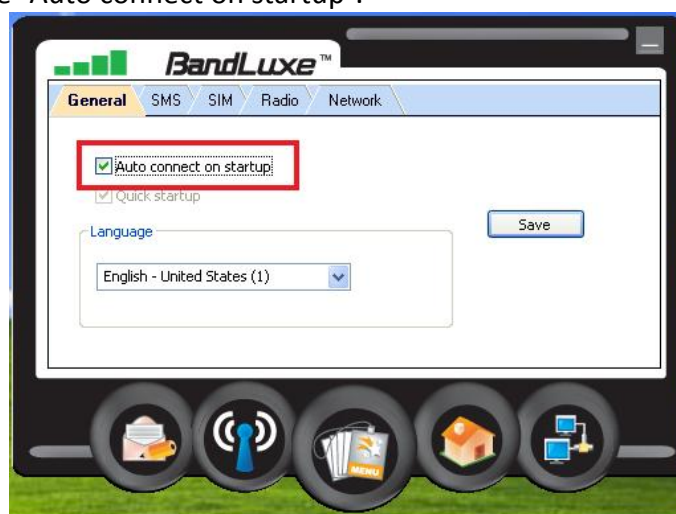
12. The utility of C100S will start up automaticity.
Please select the “MENU”



13. Click “Setting”.



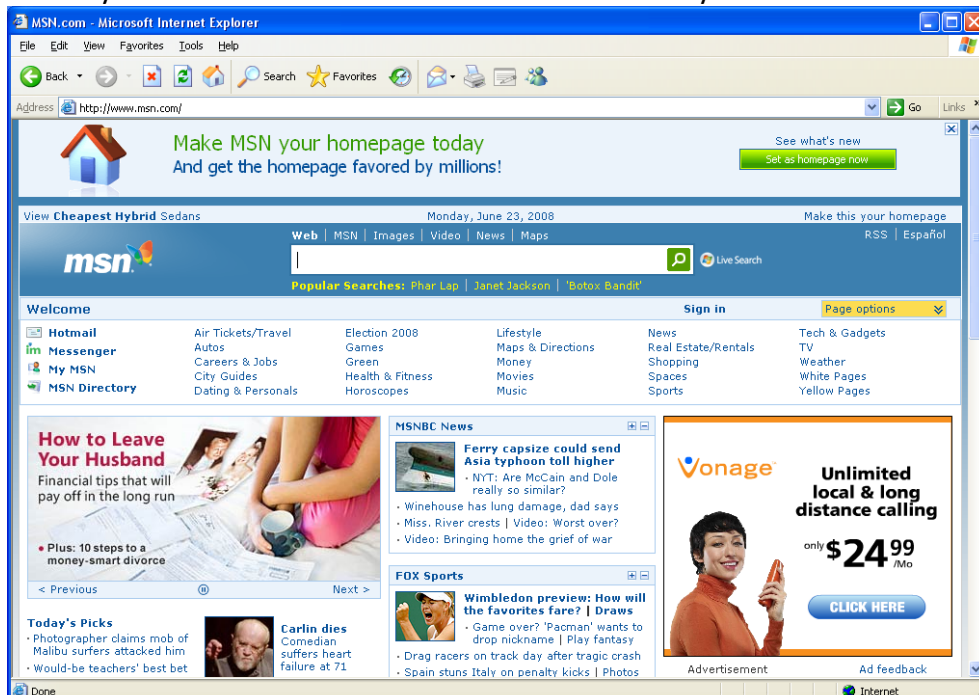
14. Select the “Auto connect on startup”.



15. Plug in the C100S into the USB port of the 3G router.
16. The USB adapter will get the IP address from ISP automatically. You can check the Status of the 3G-6200n on the Web site (ex: 192.168.2.1).



17. Now you are able to connect to Internet successfully.



Note : If your SIM card requires entering the PIN code, please enter into the web management of the 3G router. In WAN setting web page, select 3G/3.5G. Enter the PIN code of the adapter.

Please input User name & Password in “PPP Settings” and do not input them in “Network Settings” unless your ISP ask you input them in both.

| | |
|--|---------------------------------------|
| PPP Settings : | |
| Username : | <input type="text"/> |
| Password : | <input type="password"/> |
| Idle Timeout : | <input type="text" value="0"/> |
| Echo Timeout : | <input type="text" value="60"/> |
| Echo Count : | <input type="text" value="3"/> |
| Network Settings : | |
| User Name | <input type="text"/> (Optional) |
| Password | <input type="password"/> (Optional) |
| Enter PIN Code | <input type="text"/> |
| APN | <input type="text" value="internet"/> |
| Service | 3G/3.5G Only (UMTS/HSPA/HSDPA) ▼ |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

Step 3) Broadband Type (Connect to Internet via Ethernet)

3G-6200n provides two types of Internet connection method: wireless (3G/3.5G) or wired connection. You can access internet via USB 3G/3.5G modem card, or via wired xDSL / cable modem connection. However, only one connection method (wireless or wired) can be used at the same time.

In this section you have to select one of six types of connections that you will be using to connect your broadband router's WAN port to your ISP (see screen below).

Note: Different ISP's require different methods of connecting to the Internet, please check with your ISP as to the type of connection it requires.

The screenshot shows the 'Quick Setup' tab selected in the top navigation bar. On the left, a sidebar lists three steps: 1. Time Zone, 2. WAN Type, and 3. IP Address Info (which is highlighted). The main content area is titled '3G/3.5G' and lists several connection options, each with a radio button and a description:

- 3G/3.5G**: If you connect to Internet using an 3G/3.5G handset or 3G/3.5G USB modem, then you should choose this option and enter the required information.
- Cable Modem**: A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Wireless Router will automatically establish a connection, so you probably do not need to enter anything more.
- Fixed-IP xDSL**: Some xDSL Internet Service Providers may assign a Fixed IP Address for your Wireless Router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Wireless Router.
- PPPoE xDSL**: If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.
- PPTP xDSL**: If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. You must choose this option and enter the required information.
- L2TP xDSL**

| Menu | Description |
|------------------|--|
| Cable Modem | Your ISP will assign you with an IP address automatically |
| Fixed-IP xDSL | Your ISP gave you an IP address already |
| PPPoE xDSL | Your ISP requires you to use Point-to-Point Protocol over Ethernet (PPPoE) |
| PPTP xDSL | Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) |
| L2TP xDSL | Your ISP requires you to use a Layer Two Tunneling Protocol (L2TP) |
| Telstra Big Pond | This Protocol only used for Telstra Big Pond Internet service in Australia |

Click on one of the WAN type and then proceed to the manual's relevant sub-section (1.1, 1.2, 1.3, 1.4, 1.5 or 1.6). Click on **Back** to return to the previous screen.

1.1 Cable Modem

Choose Cable Modem if your ISP will assign you with an IP address automatically (**i.e. DHCP**). Some ISP's may also require that you fill in additional information such as host name and MAC address (see screen below).

Note: The Host Name and MAC address section is *optional* and you can skip this section if your ISP does not require these settings.

Dynamic IP

Cable Modem

Host Name :

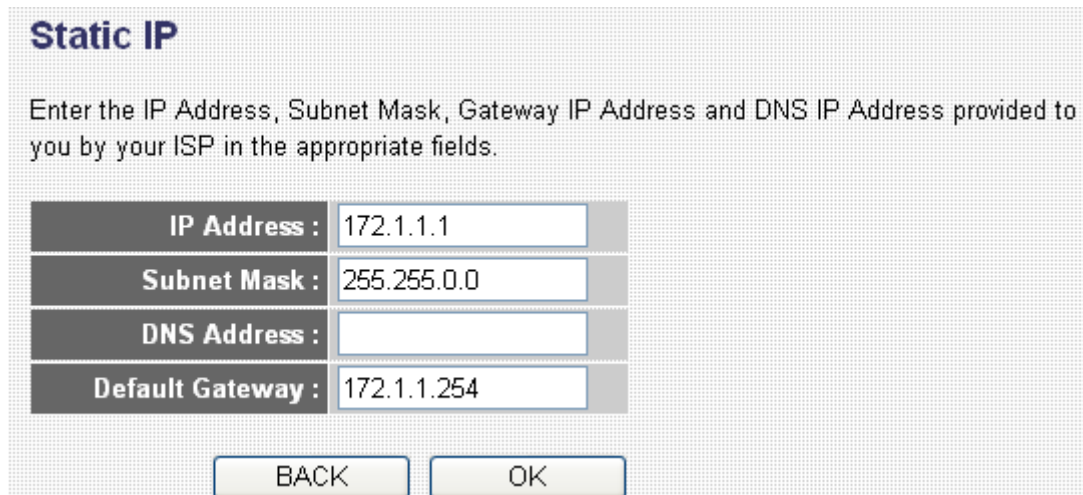
MAC Address :

| Parameters | Description |
|-------------|---|
| Host Name | If your ISP requires a Host Name, type in the host name provided by your ISP, otherwise leave it blank if your ISP does not require a Host Name. |
| MAC Address | Your ISP may require a particular MAC address to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address) |

Click **<OK>** when you have finished the configuration above. Congratulations! You have completed the configuration for the Cable Modem connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.2 Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section.



Static IP

Enter the IP Address, Subnet Mask, Gateway IP Address and DNS IP Address provided to you by your ISP in the appropriate fields.

| | |
|-------------------|-------------|
| IP Address : | 172.1.1.1 |
| Subnet Mask : | 255.255.0.0 |
| DNS Address : | |
| Default Gateway : | 172.1.1.254 |

BACK OK

| Parameters | Description |
|--------------------|---|
| IP address | This is the IP address that your ISP has given you. |
| Subnet Mask | Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0) |
| DNS address | This is the ISP's DNS server IP address |
| Gateway IP address | This is the ISP's IP address gateway |

Click <OK> when you have finished the configuration above. Congratulations! You have completed the configuration for the Fixed-IP x DSL connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3,

1.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

PPPoE

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.

| | |
|-------------------|--|
| User Name : | <input type="text"/> |
| Password : | <input type="password"/> |
| Service Name : | <input type="text"/> |
| MTU : | <input type="text" value="1392"/> (512<=MTU<=1492) |
| Connection Type : | <input type="button" value="Continuous"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/> |
| Idle Time Out : | <input type="text" value="10"/> (1-1000 Minute) |

| Parameter | Description |
|-----------------|--|
| User Name | Enter the User Name provided by your ISP for the PPPoE connection |
| Password | Enter the Password provided by your ISP for the PPPoE connection |
| Service Name | This is optional. Enter the Service name of your ISP when your ISP requires it, otherwise leave it blank. |
| MTU | This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set the maximum packet size. Please ask your ISP for detailed information. |
| Connection Type | If you select "Continuous", the router will maintain the connection to the ISP. If the WAN connection drops, the router will reconnect to the ISP automatically. If you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will drop the WAN connection if the time period that no one is using the |

| | |
|-----------|---|
| | <p>Internet exceeds the “Idle Time”.</p> <p>If you select “Manual”, the router will connect to ISP only when you click “Connect” manually from the Web management interface. The WAN connection will not disconnect because of idle timeout. If the WAN line drops and connected at a latter time again, the router will not connect to the ISP by itself.</p> |
| Idle Time | <p>You can specify an idle time (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection to your ISP.</p> <p>Note: This “idle timeout” function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends data to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially when your ISP charge you by the connection time.</p> |

Click <**OK**> when you have finished the configuration above. Congratulations! You have completed the configuration for the PPPoE connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

PPTP

Point-to-Point Tunneling Protocol is a common connection method used in xDSL connections.

• WAN Interface Settings

☒ Obtain an IP Address Automatically

| | |
|---------------|--|
| Host Name : | <input type="text"/> |
| MAC Address : | <input type="text" value="000000000000"/> <input type="button" value="Clone MAC"/> |

☐ Use The Following IP Address

| | |
|-------------------|--------------------------------------|
| IP Address : | <input type="text" value="0.0.0.0"/> |
| Subnet Mask : | <input type="text" value="0.0.0.0"/> |
| Default Gateway : | <input type="text" value="0.0.0.0"/> |

• PPTP Settings

| | |
|-------------------|--|
| User Name : | <input type="text"/> |
| Password : | <input type="password"/> |
| PPTP Gateway : | <input type="text" value="0.0.0.0"/> |
| Connection ID : | <input type="text"/> (Optional) |
| MTU : | <input type="text" value="1392"/> (512<=MTU<=1492) |
| BEZEQ-ISRAEL : | <input type="checkbox"/> Enable (For BEZEQ network in ISRAEL use only) |
| Connection Type : | <input type="text" value="Continuous"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/> |
| Idle Time Out : | <input type="text" value="10"/> (1-1000 Minute) |

| Parameter | Description |
|------------------------------|--|
| Obtain an IP address | The ISP requires you to obtain an IP address by DHCP automatically before connecting to the PPTP server. |
| Use the following IP Address | The ISP gave you a static IP to be used to connect IP address to the PPTP server |
| IP Address | This is the IP address that your ISP gave you to |

| | |
|-----------------|---|
| | establish a PPTP connection |
| Subnet Mask | Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0) |
| Gateway | Enter the IP address of the ISP's Gateway |
| User ID | Enter the User Name provided by your ISP for the PPTP connection. Sometimes called as Connection ID |
| Password | Enter the Password provided by your ISP for the PPTP connection |
| PPTP Gateway | If your LAN has a PPTP gateway, then enter that PPTP gateway's IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address, same as above |
| Connection ID | This is the ID given by your ISP, and this is optional. |
| BEZEQ-ISRAEL | Select this item if you are using the service provided by BEZEQ in Israel. |
| Connection Type | <p>If you select "Continuous", the router will maintain the connection to the ISP. If the WAN line breaks down and links again at a latter time, the router will reconnect to the ISP automatically; if you select "Connect On Demand", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time".</p> <p>If you select "Manual", the router will connect to ISP only when you click "Connect" manually from the Web management interface. The WAN connection will not be disconnected because of idle timeout. If the WAN line breaks down and got connected again at a latter time, the router will not connect to the ISP by itself.</p> |
| Idle Time | <p>You can specify an idle time threshold (minutes) for the WAN port. This means if no packets has been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection to your ISP.</p> <p>Note: This "idle timeout" function may not work due to abnormal activities of some network application</p> |

| | |
|--|--|
| | software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used |
|--|--|

Click **<OK>** when you have finished the configuration above. Congratulations! You have completed the configuration for the PPTP connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

• WAN Interface Settings

☒ Obtain an IP Address Automatically

Host Name :

MAC Address :

☐ Use The Following IP Address

IP Address :

Subnet Mask :

Default Gateway :

• L2TP Settings

User Name :

Password :

L2TP Gateway :

MTU : (512<=MTU<=1492)

Connection Type :

Idle Time Out : (1-1000 Minute)

| Parameter | Description |
|--------------|---|
| Obtain an IP | The ISP requires you to obtain an IP address by |

| | |
|------------------------------|---|
| address | DHCP automatically before connecting to the L2TP server. |
| MAC Address | Your ISP may require a particular MAC address to connect to the Internet. This MAC address is the PC's MAC address that you originally made your Internet connection. Type in this MAC address in this section or use the "Clone MAC Address" button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work). To find out the PC's MAC address see Appendix A. (see Glossary for an explanation on MAC address) |
| Use the following IP Address | The ISP gave you a static IP to be used to connect to the L2TP server. |
| IP Address | This is the IP address that your ISP has given you to establish a L2TP connection. |
| Subnet Mask | Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0) |
| Gateway | Enter the IP address of the ISP Gateway |
| User ID | Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID |
| Password | Enter the Password provided by your ISP for the PPTP connection |
| L2TP Gateway | If your LAN has a L2TP gateway, then enter that L2TP gateway IP address here. If you do not have a L2TP gateway then enter the ISP's Gateway IP address above |
| MTU | This is optional. You can specify the maximum size of your transmission packet to the Internet. Keep default value if you do not wish to set a maximum packet size. |
| Connection Type | If you select "Continuous", the router will maintain the connection to the ISP. If the WAN line breaks down and links again at a latter time, the router will auto-reconnect to the ISP. If you select "Connect On Demand", the router will connect to the ISP automatically when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "Manual", the |

| | |
|---------------|---|
| | <p>router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not be disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not connect to the ISP by itself.</p> |
| Idle Time Out | <p>The WAN "idle timeout" auto-disconnect function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. This function also may not work with some ISP. So please make sure this function can work properly when you use this function in the first time, especially your ISP charge you by time used. Due to the many uncontrollable issues, we do not guarantee the WAN "idle timeout" auto-disconnect function will always work. In order to prevent from extra connection fee, please TURN OFF THE ROUTER WHEN YOU ARE NOT USING INTERNET.</p> |

Click **<OK>** when you have finished the configuration above. Congratulations! You have completed the configuration for the L2TP connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

1.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia.

Telstra Big Pond

If your Internet service is provided by Telstra Big Pond in Australia, you will need to enter your information below. This information is provided by Teistra BigPond.

| | |
|---|--------------------------------------|
| User Name : | <input type="text"/> |
| Password : | <input type="password"/> |
| <input type="checkbox"/> Assign login server manually | |
| Server IP Address : | <input type="text" value="0.0.0.0"/> |
| <div>BACKOK</div> | |

| Parameter | Description |
|-----------------------------------|--|
| User Name | Enter the User Name provided by your ISP for the Telstra Big Pond connection |
| Password | Enter the Password provided by your ISP for the Telstra Big Pond connection |
| User decide login server manually | Select if you want to assign the IP of Telstra Big Pond's login server manually. |
| Login Server | The IP of the Login Server. |

Click **<OK>** when you have finished the configuration above. Congratulations! You have completed the configuration for the Telstra Big Pond connection. You can start using the router now, if you wish to use some of the advance features supported by this router see chapter 2, 3, 4.

Chapter 2

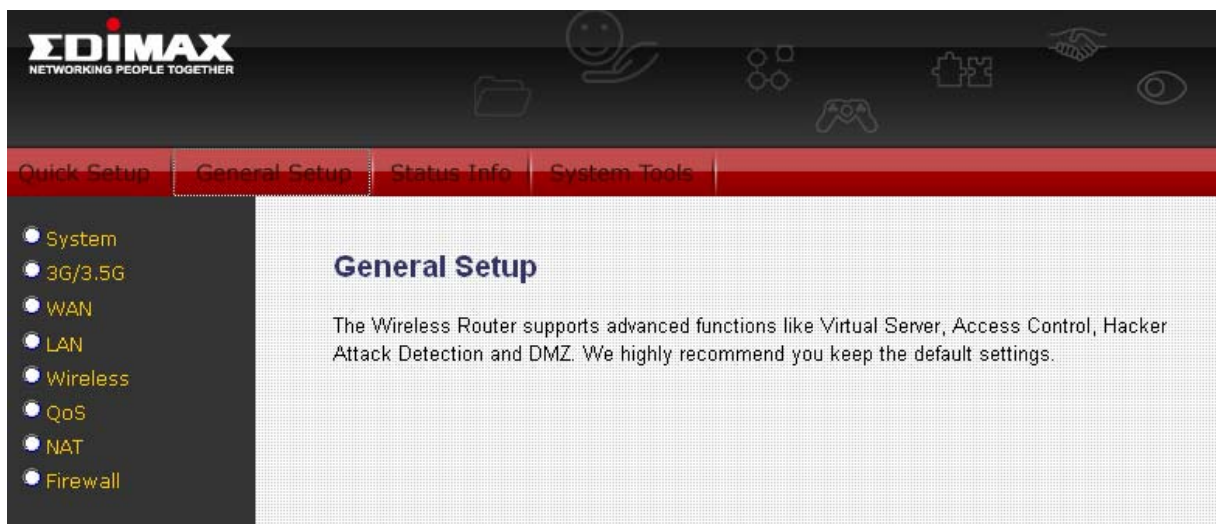
General Settings

Once you click on the **General Setup** button at the Home Page, you should see the screen below.

If you have already configured the Quick Setup Wizard, you **DO NOT** need to configure anything thing in the General Setup screen for you to start using the Internet.

The General Setup contains advanced features that allow you to configure the router to meet your network's needs such as: Wireless, Address Mapping, Virtual Server, Access Control, Hacker Attack Prevention, Special Applications, DMZ and other functions.

Below is a general description of what advance functions are available in this broadband router.



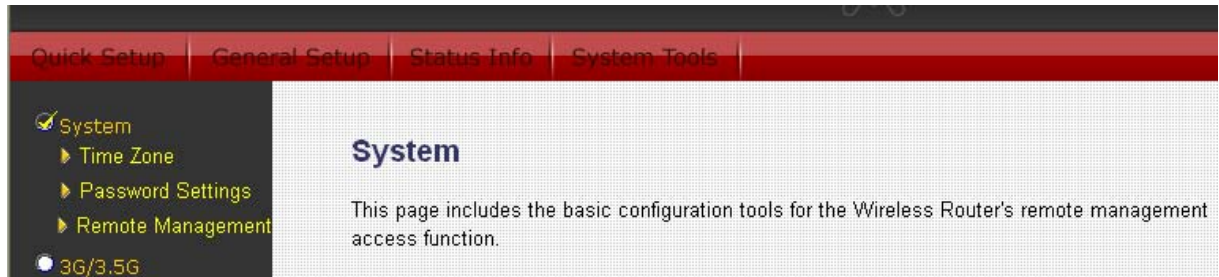
| Menu | Description |
|---------|---|
| System | This section allows you to set the Broadband router's system time zone, password and remote management administrator. |
| 3G/3.5G | This section allows you to set Internet Connection via wireless 3G USB modem. |
| WAN | This section allows you to select the connection method in order to establish a connection with your ISP (same as the Quick Setup Wizard section) |
| LAN | You can specify the LAN segment's IP address, subnet Mask, enable/disable DHCP and select an IP |

| | |
|----------|---|
| | range for your LAN |
| Wireless | Setup the wireless LAN's SSID, WEP key, MAC filtering. |
| QoS | You can setup the QoS bandwidth control policy. |
| NAT | You can configure the Address Mapping, Virtual Server and Special Applications functions in this section. This allows you to specify what user/packet can pass your router's NAT. |
| Firewall | The Firewall section allows you to configure Access Control, Hacker Prevention and DMZ. |

Select one of the above General Setup selections and proceed to the manual's relevant sub-section

2.1 System

The system screen allows you to specify a time zone, to change the system password and to specify a remote management user for the broadband router.



| Parameters | Description |
|-------------------|--|
| Time Zone | Select the time zone of the country you are living. The router will set its time based on your selection |
| Password Settings | Allows you to define a password in order to access the web-based management website. |
| Remote Management | You can specify a Host IP address that can perform remote management functions. |

Select one of the above three system settings selections and proceed to the manual's relevant sub-section

2.1.1 Time Zone

The Time Zone allows your router to reference or base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.

Time Zone ⓘ

Set the time zone of the Wireless Router. This information is used for log entries and firewall settings.

Time Zone : (GMT+00:00)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼

Time Server Address : 192.43.244.18

Daylight Savings : ☐ Enable
Time From January 1 To January 1

APPLY CANCEL

| Parameter | Description |
|---------------------|--|
| Set Time Zone | Select the time zone of the country you are living. The router will set its time based on your selection. |
| Time Server Address | The router default the “Time Server Address” is “192.43.244.18” |
| Daylight Savings | The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below). |
| Times From | Select the period in which you wish to start using daylight Saving. |
| Times to | Select the period in which you wish to stop using daylight Saving. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.1.2 Password Settings

You can change the password required to log into the broadband router's system web-based management. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

Password Settings

You can change the password required while logging into the wireless router's web-based management system. By default, the password is 1234. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 30 alphanumeric characters, and are case sensitive.

| | |
|--------------------|----------------------|
| Current Password : | <input type="text"/> |
| New Password : | <input type="text"/> |
| Confirm Password : | <input type="text"/> |

| Parameters | Description |
|--------------------|---|
| Current Password | Enter your current password for the remote management administrator to login to your Broadband router. Note: By default there is NO password |
| New Password | Enter your new password |
| Confirmed Password | Enter your new password again for verification purposes Note: If you forget your password, you'll have to reset the router to the factory default (No password) with the reset button (see router's back panel) |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.


2.1.3 Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Remote Management ?

The remote management function allows you to designate a host in the Internet to have management/configuration access to the Wireless Router from a remote site. Enter the designated host IP Address in the Host IP Address field.

| Host Address | Port | Enable |
|--------------------------------------|-----------------------------------|--------------------------|
| <input type="text" value="0.0.0.0"/> | <input type="text" value="8080"/> | <input type="checkbox"/> |

| Parameters | Description |
|--------------|---|
| Host Address | <p>This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. This means if you are at home and your home IP address has been designated the Remote Management host IP address for this router (located in your company office), then you'll be able to configure this router from your home. If the Host Address is 0.0.0.0, means anyone can access the router's web-based configuration from a remote location, if they know the password.</p> <p>Click the Enabled box to enable the Remote Management function.</p> <p>Note: When you want to access the web-based management from a remote computer, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by colon and port number 8080, e.g. 10.0.0.1:8080 (see below). You'll also need to know the password set in the Password Setting screen in order to access the router's web-based management.</p>  |

| | |
|---------|--|
| Port | The port number of remote management web interface. |
| Enabled | Select “Enabled” to enable the remote management function. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advanced functions or start using the router (with the advanced settings in place)

2.2 3G/3.5G

3G-6200n provides two types of Internet connection method: wireless (3G/3.5G) or wired connection. You can access internet via USB 3G/3.5G modem card, or via wired xDSL / cable modem connection. However, only one connection method (wireless or wired) can be used at the same time. Related instructions will be given as follow.

3G-6200n supports most of 3G/3.5G modem cards, just connect the modem card to the USB port of 3G-6200n and 3G-6200n will recognize it automatically, no additional setup procedure required. However, some of modem cards require PIN code or account / password (you have to use 3G-6200n's web interface to input these information), and some modem cards requires you to connect the modem card with your PC and install driver / utility before you connect it with 3G-6200n (all PCs which need to access Internet by 3G-6200n requires to perform this procedure once). If you still not able to connect to Internet, please use wired Internet connection to access our website :<http://www.edimax.com/> ,download latest version of firmware and upgrade 3G-6200n's firmware. If you still not be able to get connected by your 3G/3.5G modem card, please contact your dealer of purchase and provide the model name of the 3G/3.5G modem card you have, we'll try our best to help you to solve the problem.

Only one Internet connection (wireless / wired) can be used at the same time. Wireless connection (3G/3.5G) will be selected first, and use wired Internet connection as backup. Therefore, please DO NOT connect your 3G/3.5G modem card with 3G-6200n, or your telecomm service provider may charge you with high communication fee. For example, if you connect 3G/3.5G modem card with 3G-6200n when you're using wired Internet connection, wired connection will be dropped and use 3G/3.5G wireless connection instead. If 3G/3.5G wireless signal reception is poor and the connection can not be restored within 60 seconds, 3G-6200n will use wired Internet connection again, and will not switch back to wireless Internet connection (This only happens with wired Internet connection is available. If wired connection is unavailable, 3G-6200n will try to establish 3G/3.5G wireless connection again and again). If you want to use 3G/3.5G wireless connection again, you need to remove 3G/3.5G modem card from 3G-6200n and reconnect it back after 5 seconds.

(A) Plug and play, no setup procedure required.

Connect the USB 3G/3.5G modem card with 3G-6200n and make sure the corresponding USB LED indicator of 3G-6200n lights up, then you can use the web browser to access Internet.

(B) PIN code or user name / password required:

Please check the authentication method you want to use. Most of telecomm service providers require you to input PIN Code, please check 'SIM' and input the PIN code provided by telecomm service provider. Most of options listed here are optional and you don't have to provide those information if telecomm service provider doesn't provide you with those information.

If telecomm provider provides you with username / password, please check /User Name / Password box and input the user name / password provided by telecomm service provider, then click 'APPLY' button. Wait for 1 minute (for 3G-6200n to reboot)

The screenshot shows a web-based configuration interface for a router. At the top, there are four tabs: 'Quick Setup', 'General Setup', 'Status Info', and 'System Tools'. On the left side, there is a vertical menu with several options: 'System', '3G/3.5G' (which is selected and highlighted in yellow), 'WAN', 'LAN', 'Wireless', 'QoS', 'NAT', and 'Firewall'. The main content area is titled '3G/3.5G' and contains the following text: 'Your service provider settings will be detected automatically. If the settings are not the same as defaults, please enter the Authentication Method, User Name, Password, APN, PIN Code and Dialed Number provided to you by your ISP in the appropriate fields.'

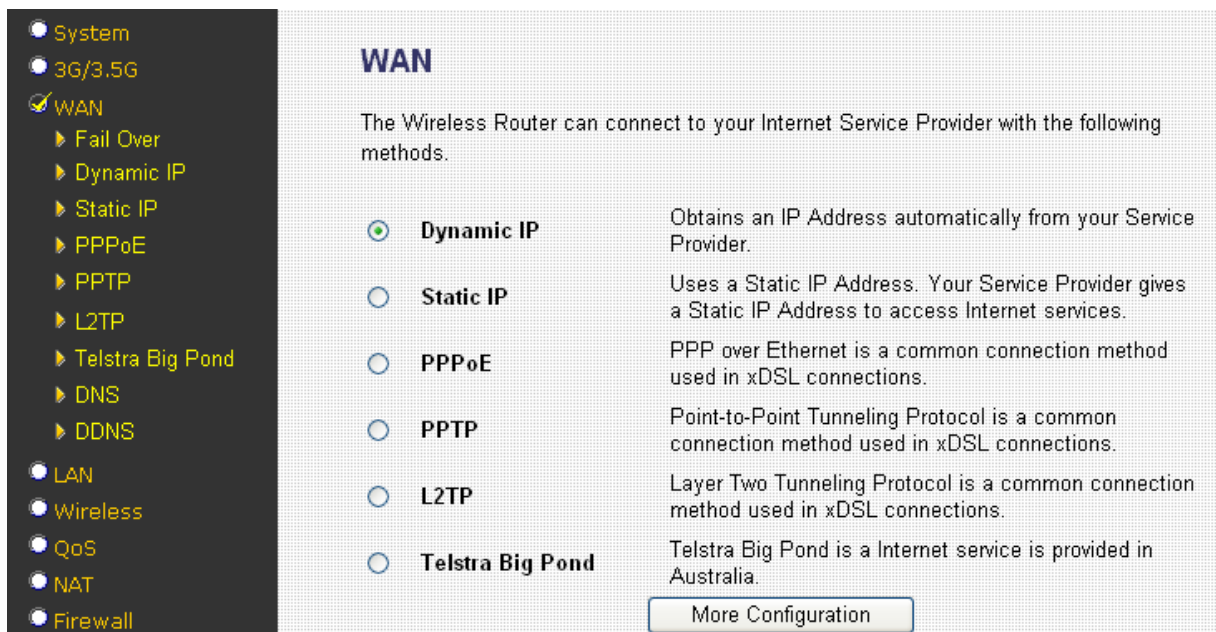
Below this text, there are two sections of settings:

- Network Settings :**
 - User Name :
 - Password :
 - PIN Code :
 - APN :
 - Dialed Number :
- Advanced PPP Settings :**
 - Username :
 - Password :
 - Service : (dropdown menu)
 - Idle Timeout :
 - Echo Timeout :
 - Echo Count :

At the bottom of the settings area, there are two buttons: 'Apply' and 'Cancel'.

2.3 WAN

Use the WAN Settings screen if you have already configured the Quick Setup Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows to specify the type of WAN port connect you want to establish with your ISP. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP, Static IP Address, PPPoE, PPTP, L2TP, Telstra Big Pond, DNS and DDNS.**



| Parameters | Description |
|------------------|--|
| Dynamic IP | Your ISP will assign you an IP address automatically |
| Static IP | Your ISP gave you an IP address already |
| PPPoE | Your ISP requires PPPoE connection. |
| PPTP | Your ISP requires you to use Point-to-Point Tunneling Protocol (PPTP) connection. |
| L2TP | Your ISP requires L2TP connection. |
| Telstra Big Pond | Your ISP requires Telstra Big Pond connection. |
| DNS | You can specify a DNS server that you wish to use |
| DDNS | You can specify a DDNS server that you wish to use and configure the user name and password provided by you DDNS service provider. |

Once you have made a selection, click **<More Configuration>** at the bottom of the screen and proceed to the manual's relevant sub-section

2.3.1 Dynamic IP

Choose the Dynamic IP selection if your ISP will assign you an IP address automatically. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address (see chapter 1 "Cable Modem" for more detail)

2.3.2 Static IP Address

Select Static IP address if your ISP assigned you with a specific IP address for you to use. Your ISP should provide all the information required in this section. (See chapter 1 “Fixed IP” for more detail)

2.3.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 “PPPoE” for more detail)

2.3.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 “PPTP” for more detail)

2.3.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. (See chapter 1 “L2TP” for detailed information)

2.3.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect to the Internet. Your ISP should provide all the information required in this section. Telstra Big Pond protocol is used by the ISP in Australia. (See chapter 1 “Telstra Big Pond” for more detail)

2.3.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify the IP address of that DNS server here.

A DNS (Domain Name System) server is like an index of IP Addresses and Web Addresses. If you type a Web address into your browser, such as www.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.

| | |
|---|----------------------|
| Primary DNS : | <input type="text"/> |
| Secondary DNS : | <input type="text"/> |
| <div><input type="button" value="APPLY"/> <input type="button" value="CANCEL"/></div> | |

| Parameters | Description |
|----------------------------------|--|
| DNS address | Fill in the ISP's DNS server IP address; or you can specify your own preferred DNS server IP address |
| Secondary DNS Address (optional) | This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used when the above DNS fail. |


Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router (with the advanced settings in place)

2.3.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain

name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.

DDNS (DynamicDNS) allows users to map the static domain name to a dynamic IP address. You must get a account, password and your static domain name from the DDNS service providers. Our products have DDNS support for www.dyndns.org and www.tzo.com now.

| | |
|-------------------------|--|
| Dynamic DNS : | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Provider : | DynDNS  |
| Domain Name : | <input type="text"/> |
| Account : | <input type="text"/> |
| Password / Key : | <input type="text"/> |

| Parameters | Default | Description |
|----------------|---------|---|
| Enable/Disable | Disable | Enable/Disable the DDNS function of this router |
| Provider | | Select a DDNS service provider |
| Domain name | | Your static domain name that use DDNS |
| Account/E-mail | | The account that your DDNS service provider assigned to you |
| Password/Key | | The password you set for the DDNS service account above |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.4 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.

You can enable the Wireless Router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The Wireless Router must have an IP Address in the Local Area Network.

- **LAN IP**

| | |
|------------------------|---------------|
| IP Address : | 192.168.2.1 |
| Subnet Mask : | 255.255.255.0 |
| 802.1d Spanning Tree : | Disable ▾ |
| DHCP Server : | Enable ▾ |
- **DHCP Server**

| | |
|------------------------|---------------|
| Lease Time : | Forever ▾ |
| DHCP Client Start IP : | 192.168.2.100 |
| DHCP Client End IP : | 192.168.2.200 |
| Domain Name : | |

APPLY CANCEL

- **Static DHCP Lease Table** It allows 16 entries only.

| NO. | MAC Address | IP Address | Select |
|-------------------|-------------|------------|--------|
| Delete Delete All | | | |
- ☐ **Enable Static DHCP Leases**

| MAC Address | IP Address |
|-------------|------------|
| | |
| Add Clear | |

| Parameters | Default | Description |
|----------------|---------------|--|
| IP address | 192.168.2.1 | This is the router's LAN port IP address (Your LAN clients default gateway IP address) |
| IP Subnet Mask | 255.255.255.0 | Specify a Subnet Mask for your LAN |

| | | |
|----------------------|----------|--|
| | | segment |
| 802.1d Spanning Tree | Disabled | If 802.1d Spanning Tree function is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports. |
| DHCP Server | Enabled | You can enable or disable the DHCP server. By enabling the DHCP server the router will automatically give your LAN clients an IP address. If the DHCP is not enabled then you'll have to manually set your LAN client's IP addresses; make sure the LAN Client is in the same subnet as this broadband router if you want the router to be your LAN client's default gateway |
| Lease Time | | When enabled, DHCP service will temporarily give your LAN clients an IP address. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time period is reached |
| IP Address Pool | | You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. Note: By default the IP range is from: 192.168.2.100 to 192.168.2.200 . If you want your PC to have a static/fixed IP address then you'll have to choose an IP address outside this IP address Pool. |
| Domain Name | | You can specify a Domain Name for your LAN. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5 Wireless

Wireless Access Point builds a wireless LAN and can let all PCs equipped with IEEE 802.11b or 801.11g wireless network adaptor connect to your Intranet. It supports WEP and WPA2 encryption to enhance the security of your wireless network.



| Parameters | Default | Description |
|--|---------|--|
| Enable or disable Wireless module function | Enable | You can select to enable or disable the wireless access point module of this router. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.1 Basic Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

| | |
|------------------------------------|---------------------|
| Mode : | Access Point |
| Band : | 2.4 GHz (B+G+N) |
| SSID : | uuuuuuu |
| Channel Number : | 11 |
| Associated Clients : | Show Active Clients |
| <div>APPLY</div> <div>CANCEL</div> | |

| Parameters | Default | Description |
|----------------|---------|--|
| Mode | | It allows you to set the AP to AP, Bridge or WDS mode. |
| Band | | It allows you to select the wireless band: 802.11(B+G+N),802.11(B+G),802.11b and / or 802.11g. You can select B+G+N mode to allow all 802.11b,802.11g and 802.11n clients to connect to this wireless access point. |
| ESSID | default | This is the name of the wireless access point. All devices in the same wireless LAN should have the same ESSID. |
| Channel Number | 11 | The wireless channel used by the wireless access point. All devices in the same wireless LAN should use the same channel. |
| MAC address | | If you want to combine more than one network, you have to set this access point to "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" or "AP Bridge-WDS mode". You have to enter the MAC addresses of other access points which will join the same wireless network. |
| Set Security | | Click the "Set Security" button, and then a |

| | | |
|--|--|---|
| | | <p>“WDS Security Settings” will pop up. You can set the security parameters used to bridge access points together here, when you set your AP in AP Bridge mode. You can refer to section 4.3 “Security Settings” for detailed instructions.</p> |
|--|--|---|

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advanced sections or start using the router (with the advanced settings in place)

2.5.2 Advanced Settings

You can set advanced wireless LAN parameters of this router. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, preamble Type, etc. You should not change these parameters unless you know their function and effects.

| | | |
|----------------------|---|--|
| Fragment Threshold : | <input type="text" value="2346"/> | (256-2346) |
| RTS Threshold : | <input type="text" value="2347"/> | (0-2347) |
| Beacon Interval : | <input type="text" value="100"/> | (20-1000 ms) |
| DTIM Period : | <input type="text" value="3"/> | (1-10) |
| Data Rate : | <input type="button" value="Auto"/> | |
| N Data Rate : | <input type="button" value="Auto"/> | |
| Channel Width : | <input checked="" type="radio"/> Auto 20/40 MHz | <input type="radio"/> 20 MHz |
| Preamble Type : | <input checked="" type="radio"/> Short Preamble | <input type="radio"/> Long Preamble |
| Broadcast Essid : | <input checked="" type="radio"/> Enable | <input type="radio"/> Disable |
| CTS Protect : | <input type="radio"/> Auto | <input type="radio"/> Always <input checked="" type="radio"/> None |
| Tx Power: | <input type="button" value="100 %"/> | |
| WMM: | <input type="radio"/> Enable | <input checked="" type="radio"/> Disable |

| Parameters | Description |
|--------------------|--|
| Fragment Threshold | "Fragment Threshold" specifies the maximum fragmentation size of data packet to be transmitted. If this value is too low, it will result in bad performance. |
| RTS Threshold | When the packet size is smaller the RTS threshold, the wireless access point will not use the RTS/CTS mechanism to send this packet. |
| Beacon Interval | The interval of time that this wireless access point broadcast a beacon. Beacon is used to synchronize the wireless network. |
| DTIM Period | The DTIM period you specify here indicates how often the clients served by this access point should check for buffered data which still exists on the AP |

| | |
|-----------------|---|
| | and waiting for pickup. |
| Data Rate | The “Data Rate” is the rate this access point used to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets. |
| N Data Rate | We provide”MCS0~MCS7 and Auto” for configuration, and default setting is “Auto” . |
| Channel Width | The default setting is “Auto 20/40MHz”, and the default setting will provide you better wireless performance than “20MHz”. |
| Preamble Type | The “Long Preamble” can provide better wireless LAN compatibility while the “Short Preamble” can provide better wireless LAN performance. |
| Broadcast ESSID | If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point will discover this access point more easily. If you are building a wireless network which will open to the public, it’s recommended to enable this feature. Disabling “Broadcast ESSID” can provide better security. |
| CTS Protect | It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic will be transmitted. |
| Tx Power | You can adjust the wireless transmit power here. By reduce the TX power, you can reduce the wireless coverage to make it only cover the area you need. |
| WMM | WMM stands for Wi-Fi Multimedia. It is a standard created to define quality of service (QoS) in Wi-Fi networks. This adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3 Security

This Router provides complete wireless LAN security functions, include WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

2.5.3.1 WEP only

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the router can receive any packets encrypted by one of the four keys.

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| | |
|---|---------------------|
| Encryption : | WEP |
| Key Length : | 64-bit |
| Key Format : | Hex (10 Characters) |
| Default Tx Key : | Key 1 |
| Encryption Key 1 : | ***** |
| Encryption Key 2 : | ***** |
| Encryption Key 3 : | ***** |
| Encryption Key 4 : | ***** |
| <input type="checkbox"/> Enable 802.1x Authentication | |
| <div>APPLY</div> <div>CANCEL</div> | |

| Parameters | Default | Description |
|------------|---------|---|
| Key Length | 64-bit | You can select the WEP key length for encryption, 64-bit or 128-bit. Larger WEP key length will provide higher level of security, but the data throughput will be lowered. |
| Key Format | | You can select ASCII Characters (alphanumeric format) or Hexadecimal Digits ("A-F", "a-f" and "0-9") to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde |

| | | |
|------------------|--|--|
| Default Key | | Select one of the four keys to encrypt your data. Only the key you select it in the "Default key" will be used. |
| Key 1 – Key 4 | | The WEP keys are used to encrypt data transmitted over the wireless network. Fill the text box by following the rules: 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values ("A-F", "a-f" and "0-9") or 13-digit ASCII characters as the encryption keys. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3.2 802.1x only

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication.

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| | | |
|--|-----------------------------------|--|
| Encryption : | Disable | ▼ |
| <input checked="" type="checkbox"/> Enable 802.1x Authentication | | |
| RADIUS Server IP Address : | <input type="text"/> | |
| RADIUS Server Port : | <input type="text" value="1812"/> | |
| RADIUS Server Password : | <input type="password"/> | |
| | | <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/> |

| Parameters | Description |
|--------------------------|---|
| RADIUS Server IP address | The IP address of external RADIUS server. |
| RADIUS Server Port | The service port of the external RADIUS server. |
| RADIUS Server Password | The password used by external RADIUS server. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3.3 802.1x WEP Static key

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication.

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| | |
|--|---------------------|
| Encryption : | WEP |
| Key Length : | 64-bit |
| Key Format : | Hex (10 Characters) |
| Default Tx Key : | Key 1 |
| Encryption Key 1 : | ***** |
| Encryption Key 2 : | ***** |
| Encryption Key 3 : | ***** |
| Encryption Key 4 : | ***** |
| <input checked="" type="checkbox"/> Enable 802.1x Authentication | |
| RADIUS Server IP Address : | |
| RADIUS Server Port : | 1812 |
| RADIUS Server Password : | |
| <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/> | |

For detailed instructions of WEP settings, please refer to section 2.4.3.1 "WEP only". For the 802.1x settings, please refer to section 2.4.3.2 "802.1x only".

2.5.3.4 WPA Pre-shared key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key will not be known by hackers easily, and this will improve security.

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| | |
|----------------------------|---|
| Encryption : | WPA pre-shared key ▼ |
| WPA Unicast Cipher Suite : | <input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed |
| Pre-shared Key Format : | Passphrase ▼ |
| Pre-shared Key : | ***** |
| <div>APPLY CANCEL</div> | |

| Parameters | Description |
|-----------------------|--|
| WPA(TKIP) | TKIP will change the encryption key frequently to enhance the wireless LAN security. |
| WPA2(AES) | WPA2 AES uses CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security. |
| WPA2 Mixed | WPA2 Mixed will use TKIP or AES based on the other communication peer automatically. |
| Pre-shared Key Format | You may select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde |
| Pre-shared Key | The Pre-shared key is used to authenticate and encrypt data transmitted over the wireless network. Fill the text box by following the rules listed here: Hex WEP: input 64-digit Hex values ("A-F", "a-f" and "0-9") or at least 8 character pass phrase as the pre-shared keys. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.3.5 WPA Radius

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently, and this will improve security.

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

| | |
|--|---|
| Encryption : | WPA RADIUS |
| WPA Unicast Cipher Suite : | <input checked="" type="radio"/> WPA(TKIP) <input type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed |
| RADIUS Server IP Address : | |
| RADIUS Server Port : | 1812 |
| RADIUS Server Password : | |
| <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/> | |

| Parameters | Description |
|--------------------------|--|
| WPA(TKIP) | TKIP will change the encryption key frequently to enhance the wireless LAN security. |
| WPA2(AES) | WPA2 AES uses CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security. |
| WPA2 Mixed | WPA2 MIXED will use TKIP or AES based on the other communication peer automatically. |
| RADIUS Server IP address | The IP address of external RADIUS server. |
| RADIUS Server Port | The service port of the external RADIUS server. |
| RADIUS Server Password | The password used by external RADIUS server. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.4 Access Control

This wireless router provides MAC Address Control, which prevents unauthorized MAC Addresses from accessing your wireless network.

For security reason, the Wireless Router features MAC Address Filtering that only allows authorized MAC Addresses associating to the Wireless Router.

- **MAC Address Filtering Table**

It allows 20 entries only.

| NO. | MAC Address | Comment | Select |
|--|----------------------|----------------------|---|
| | | Delete | Delete All |
| <input type="checkbox"/> Enable Access Control | | | |
| | <input type="text"/> | <input type="text"/> | <input type="button" value="Add"/> <input type="button" value="Clear"/> |
| | | APPLY | CANCEL |

| Parameters | Description |
|--------------------------------|--|
| Enable wireless access control | Enable wireless access control |
| Add MAC address into the list | Fill in the "MAC Address" and "Comment" of the wireless station to be added and then click "Add". Then this wireless station will be added into the "Current Access Control List" below. If you find any issues before adding it and want to correct it. Just click "Clear" and both "MAC Address" and "Comment" fields will be cleared. |
| Remove MAC address from list | If you want to remove some MAC address from the "Current Access Control List ", select the MAC addresses you want to remove in the list and then click "Delete Selected". If you want remove all MAC addresses from the table, click "Delete All" button. Click "Reset" will clear your current selections. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.5.5 WPS

WPS (Wi-Fi Protected Setup) provides a convenient way to establish the connection between this broadband router and wireless clients. Any WPS-compatible wireless clients can establish secure connection with this broadband router with simple push-button type configuration or PinCode type configuration.

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). WPS can help your wireless client automatically connect to the Wireless Router.

☒ **Enable WPS**

☐ **Enable WPS Proxy**

• WPS Information

| | |
|------------------------------|--------------------|
| WPS Status : | Configured |
| PinCode Self : | 20613921 |
| SSID : | uuuuuuu |
| Authentication Mode : | WPA pre-shared key |
| Passphrase Key : | ***** |

• Device Configure

| | |
|--------------------------------------|---|
| Config Mode : | Registrar ▼ |
| Configure by Push Button : | <input type="button" value="Start PBC"/> |
| Configure by Client PinCode : | <input type="text"/> <input type="button" value="Start PIN"/> |

Here are descriptions of every setup items:


| Item Name | Description |
|----------------------|---|
| <i>Enable WPS</i> | <i>Check this box to enable WPS function, uncheck it to disable WPS.</i> |
| <i>WPS Status</i> | <i>If the wireless security (encryption) function of this wireless router is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'unConfigured'.</i> |
| <i>Self PIN code</i> | <i>This is the WPS PIN code of this wireless router. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless</i> |

| | |
|-------------------------------------|---|
| | <i>devices.</i> |
| <i>SSID</i> | <i>The SSID of this wireless router will be displayed here.</i> |
| <i>Authentication Mode</i> | <i>The wireless security authentication mode of this wireless router will be displayed here.</i> |
| <i>Passphrase Key</i> | <i>The WPA passphrase will be displayed as asterisk here.</i> |
| <i>Config Mode</i> | <p><i>Select the WPS configuration role of this broadband router.</i></p> <p><i>Registrar: This broadband router will act as WPS registrar and wait for wireless clients to send WPS configuration request.</i></p> <p><i>Enrollee: This broadband router will act as WPS enrollee and send WPS configuration request to other WPS registrar.</i></p> |
| <i>Configure via Push Button</i> | <p><i>Click 'Start PBC' to start Push-Button type WPS configuration (PBC). Please push the WPS push-button on other WPS-compatible network devices to begin WPS configuration.</i></p> <p><i>You can also push the 'WPS / Reset' button located at the back of this broadband router to start PBC without using web configuration interface.</i></p> |
| <i>Configure via Client PinCode</i> | <i>Please input the PinCode displayed at the configuration software of WPS-enabled wireless client, and click 'Start PIN' to establish connection with the wireless client.</i> |

2.6 QoS

The QoS function can classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using delay-sensitive services like Internet phone, video conference ...etc. All the applications not specified by you are classified as rule name "Others". The rule with smaller priority number has higher priority; the rule with larger priority number has lower priority. You can adjust the priority of the rules by moving them up or down.

Note: If the total assigned bandwidth of higher priority applications is larger than the maximum bandwidth provided by the WAN port, then other applications will not get any bandwidth.

QoS 

QoS (Quality of Service) refers to the capability of a network to provide better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. Also important is making sure that providing priority for one or more flows does not make other flows fail.

☐ Enable QoS

Total Download Bandwidth : ---Select--- >> kbits

Total Upload Bandwidth : ---Select--- >> kbits

Current QoS Table

| Priority | Rule Name | Upload Bandwidth | Download Bandwidth | Select |
|----------|-----------|------------------|--------------------|--------|
|----------|-----------|------------------|--------------------|--------|

| Parameters | Description |
|----------------|---|
| Enable QoS | You can check "Enable QoS" to enable QoS function for the WAN port. You also can uncheck "Enable QoS" to disable QoS function for the WAN port. |
| Total Download | Here you can set maximum download bandwidth for all the users of the router. |

| | |
|-------------------------------|--|
| Bandwidth | |
| Total Upload Bandwidth | Here you can set the maximum upload bandwidth for all the users of the router. |
| Add a QoS rule into the table | Click “Add”, and the QoS rule form will appear. Click “Apply” after filling the form and the rule will be added into the table. |
| Remove QoS rules from table | If you want to remove some QoS rules from the table, select the QoS rules you want to remove in the table and then click "Delete". If you want to remove all QoS rules from the table, just click "Delete All" button. Click "Reset" will clear your current selections. |
| Edit a QoS rule | Select the rule you want to edit and click “Edit”, then the detailed information of the selected QoS rule will appear. Click “Apply” after editing the form and the rule will be saved. |
| Adjust QoS rule priority | You can select the rule and click “Move Up” to make its priority higher. You also can select the rule and click “Move Down” to make its priority lower. |

Edit QoS Rule:

You can assign packet classification criteria by its local IP range, remote IP range, traffic type, protocol, local port range and remote port range parameters. The parameters you leave blank will be ignored. The priority of this rule will be applied to packets that match the classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.

QoS

This page allows users to add/modify the QoS rule's settings.

| | |
|---------------------|--|
| Rule Name : | <input type="text"/> |
| Bandwidth : | Download <input type="button" value="v"/> <input type="text"/> Kbps Guarantee <input type="button" value="v"/> |
| Local IP Address : | <input type="text"/> - <input type="text"/> |
| Local Port Range : | <input type="text"/> |
| Remote IP Address : | <input type="text"/> - <input type="text"/> |
| Remote Port Range : | <input type="text"/> |
| Traffic Type : | None <input type="button" value="v"/> |
| Protocol : | TCP <input type="button" value="v"/> |

| Parameters | Description |
|-------------------|--|
| Rule Name | The name of this rule. |
| Bandwidth | You can assign the download or upload bandwidth in Kbps (1024 bit per second). You can limit the maximum bandwidth consumed by this rule by selecting "Maximum". You also can reserve enough bandwidth for this rule by selecting "Guarantee". |
| Local IP Address | Enter the local IP address range of the packets that this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5 |
| Local Port Range | Enter the local port range of the packets that this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash "-", for example "101-150" means from port number 100 to port number 150 – the range of 50 port numbers. |
| Remote IP Address | Enter the remote IP address range of the packets that this rule will apply to. If you assign 192.168.2.3 – 192.168.2.5, it means 3 IP addresses: 192.168.2.3, 192.168.2.4 and 192.168.2.5 |
| Remote Port Range | Enter the remote port range of the packets that this rule will apply to. You can assign a single port number here or assign a range of port numbers by assigning the first port number and the last port number of the range. The two numbers are separated by a dash "-", for example "101-150" means from port number 101 to port number 150, which indicates 50 port numbers. |
| Traffic Type | Select the traffic type of the packets that this rule will apply to. We list some popular applications here to ease the configuration. You also can get the same result by using other parameters, for example source or destination port number, if you are familiar with the application protocol. |
| Protocol | Select the protocol type of the packets that this rule will apply to. |
| Apply | Apply and exit the form. |
| Reset | Clear the content of this form. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map private IP addresses to public IP addresses for key services such as Websites and FTP.



| Parameters | Description |
|----------------------|---|
| Port Forwarding | You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Port Forwarding function allows you to redirect a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. |
| Virtual Server | You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Virtual Server allows you to redirect a particular service port number (from the Internet/WAN Port) to a particular LAN IP address and its service port number. |
| Special Applications | Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support these types of applications. |
| UPnP Setting | It allows to enable or disable UPnP feature here. After you enable the UPnP feature, all client systems that |

| | |
|----------------|---|
| | support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAT port translation. |
| ALG Setting | You can let special applications that require "Application Layer Gateway" to be supported here. |
| Static Routing | You can disable NAT function and setup the routing rules manually. |

Click on one of the above NAT selections and proceed to the manual's relevant sub-section.

2.7.1 Port Forwarding

The Port Forwarding allows you to redirect a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ **Enable Port Forwarding**

| Private IP | Computer Name | Type | Port Range | Comment |
|------------------------------------|------------------------|------|---|--------------------------------------|
| <input type="text"/> | << -----Select----- >> | Both | <input type="text"/> - <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> | | | | <input type="button" value="Reset"/> |

• **Current Port Forwarding Table**

| NO. | Computer Name | Private IP | Type | Port Range | Comment | Select |
|-----|---------------|------------|------|---------------------------------------|---|--------------------------------------|
| | | | | <input type="button" value="Delete"/> | <input type="button" value="Delete All"/> | <input type="button" value="Reset"/> |
| | | | | <input type="button" value="APPLY"/> | <input type="button" value="CANCEL"/> | |

| Parameters | Description |
|------------------------|--|
| Enable Port Forwarding | Enable Port Forwarding |
| Private IP | This is the private IP of the server behind the NAT firewall. Note: You need to give your LAN PC clients a fixed/static IP address in order to make port forwarding function working properly. |
| Computer Name | For you to choose PC or NB. |
| Type | This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "both" to forward both "TCP" and "UDP" packets. |
| Port Range | The range of ports to be forward to the private IP. |
| Comment | The description of this setting. |
| Add Port Forwarding | Fill in the "Private IP", "Type", "Port Range" and "Comment" of the setting to be added and then click |

| | |
|------------------------|---|
| | "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you found any typo before adding it and want to correct it, just click "Clear" and the fields will be cleared. |
| Remove Port Forwarding | If you want to remove some Port Forwarding settings from the "Current Port Forwarding Table", select the Port Forwarding settings you want to remove in the table and then click "Delete Selected". If you want remove all Port Forwarding settings from the table, just click "Delete All" button. Click "Reset" will clear your current selections. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7.2 Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to redirect a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number. (See Glossary for an explanation on Port number)

You can configure the Wireless Router as a Virtual Server so that remote users accessing services such as the Web or FTP at your local site via Public IP Addresses can be automatically redirected to local servers configured with Private IP Addresses. In other words, depending on the requested service (TCP/UDP) port number, the Wireless Router redirects the external service request to the appropriate internal server (located at one of your LAN's Private IP Address).

☐ **Enable Virtual Server**

| Private IP | Computer Name | Private Port | Type | Public Port | Comment |
|------------------------------------|------------------------|----------------------|--------|----------------------|--------------------------------------|
| <input type="text"/> | << -----Select----- >> | <input type="text"/> | Both > | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> | | | | | <input type="button" value="Reset"/> |

• **Current Virtual Server Table**

| NO. | Computer Name | Private IP | Private Port | Type | Public Port | Comment | Select |
|---------------------------------------|---------------|------------|--------------|------|---|--------------------------------------|--------|
| <input type="button" value="Delete"/> | | | | | <input type="button" value="Delete All"/> | <input type="button" value="Reset"/> | |
| <input type="button" value="APPLY"/> | | | | | <input type="button" value="CANCEL"/> | | |

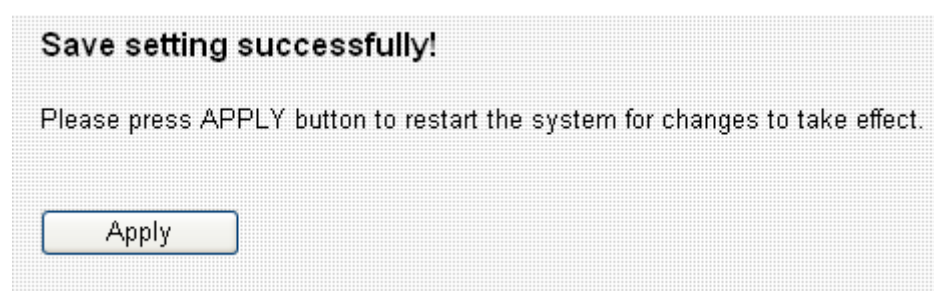
Here are descriptions of every setup items:

| Item Name | Description |
|-----------------------|---|
| Enable Virtual Server | Check this box to enable virtual server, and uncheck this box to disable virtual server. |
| Private IP | Input the IP address of the computer which provides Internet service. |
| Computer name | All computer names found by this broadband router on local network will be listed here. You can select the computer name and click '<<' button to add selected computer's IP address to 'Private IP' field. |

| | |
|---------------------|--|
| | <i>Please note that this list may not be able to list all computers on your local network.</i> |
| <i>Private Port</i> | <i>Input the port number of the IP address which provides Internet service.</i> |
| <i>Type</i> | <i>Select the type of connection, TCP or UDP. If you're not sure, please select 'Both'</i> |
| <i>Public Port</i> | <i>Please select the port number of Internet IP address which will be redirected to the port number of local IP address defined above.</i> |
| <i>Comment</i> | <i>Please input any text to describe this mapping, up to 16 alphanumerical characters.</i> |
| <i>Add</i> | <i>Add the mapping to virtual server table.</i> |
| <i>Reset</i> | <i>Remove all inputted values.</i> |

All existing virtual server mappings will be displayed in this page. To delete one or more mappings, check the box of the mapping, then click 'Delete Selected' button to remove the mapping. To delete all existing mappings, click 'Delete All' button. If you want to uncheck all boxes, click 'Reset'.

When you finished with the settings in this page, you can click 'Apply' button to save changes you made in this page, or you can click 'Cancel' to discard changes. After you click 'Apply' button, you'll see the following messages:



Please click 'Apply' to save changes you made and restart the broadband router, this requires about 30 seconds and the broadband router will stop responding (this is normal and is not malfunction). You can reconnect to this broadband router and continue on other settings later.

2.7.3 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

Special Applications ?

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic. Note: The range of the Trigger Port is 1 to 65535.

☐ Enable Special Applications

| IP Address | Computer Name | TCP Port to Open | UDP Port to Open | Comment |
|--------------------------------------|------------------------|------------------|------------------|---------|
| 0.0.0.0 | << -----Select----- >> | | | |
| Popular Applications : Select Game > | | Add | | |
| | | Add | Reset | |

• Current Trigger-Port Table

| NO. | Computer Name | IP Address | TCP Port to Open | UDP Port to Open | Comment | Select |
|-----|---------------|------------|------------------|------------------|---------|-------------------------|
| | | | | | | Delete Delete All Reset |

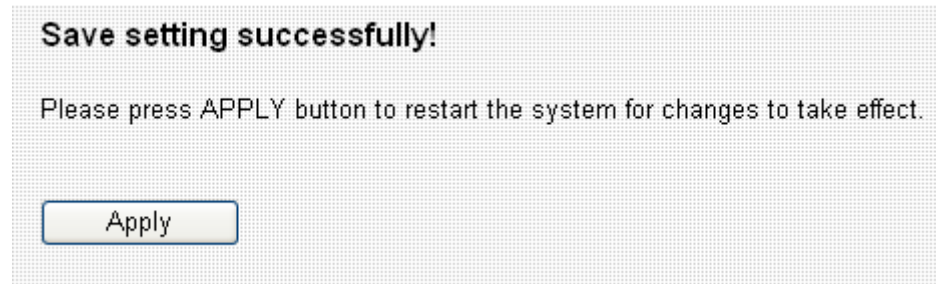
Here are descriptions of every setup items:

| Item Name | Description |
|------------------|--|
| Enable | Check this box to enable support for special applications, and uncheck this box to disable this support. |
| IP Address | Input the IP address of the computer which is going to use the special application. |
| Computer name | All computer names found by this broadband router on local network will be listed here. You can select the computer name and click '<<' button to add selected computer's IP address to 'IP Address' field. Please note that this list may not be able to list all computers on your local network. |
| TCP Port to Open | Input the TCP port number required by the special |

| | |
|--------------------------|---|
| | <i>application, the port number can be a single value, or a range (like 20-50). If you need to input more than one port number and they're not contiguous, list all port numbers here and separate them by comma (,). If the application does not use TCP port, leave it blank.</i> |
| <i>UDP Port to Open)</i> | <i>Input the UDP port number required by the special application, the port number can be a single value, or a range (like 20-50). If you need to input more than one port number and they're not contiguous, list all port numbers here and separate them by comma (,). If the application does not use UDP port, leave it blank.</i> |
| <i>Comment</i> | <i>You can input any text here to help you remember the purpose of this item. This is optional.</i> |
| <i>Select Game</i> | <i>This router comes with a numerous port mapping settings of network games. If the game you wish to set is listed here, you can select it from dropdown menu.</i> <i>After a game is selected, click 'Add' (the one next to 'Select Game' dropdown list) to add the connection parameters to all respective fields.</i> |
| <i>Add</i> | <i>Click this button to add a new port mapping rule to special applications table.</i> |
| <i>Reset</i> | <i>Click this button to remove all values in every field.</i> |

All existing special application mappings will be displayed in this page. To delete one or more mappings, check the box of the mapping, then click 'Delete Selected' button to remove the mapping. To delete all existing mappings, click 'Delete All' button. If you want to uncheck all boxes, click 'Reset'.

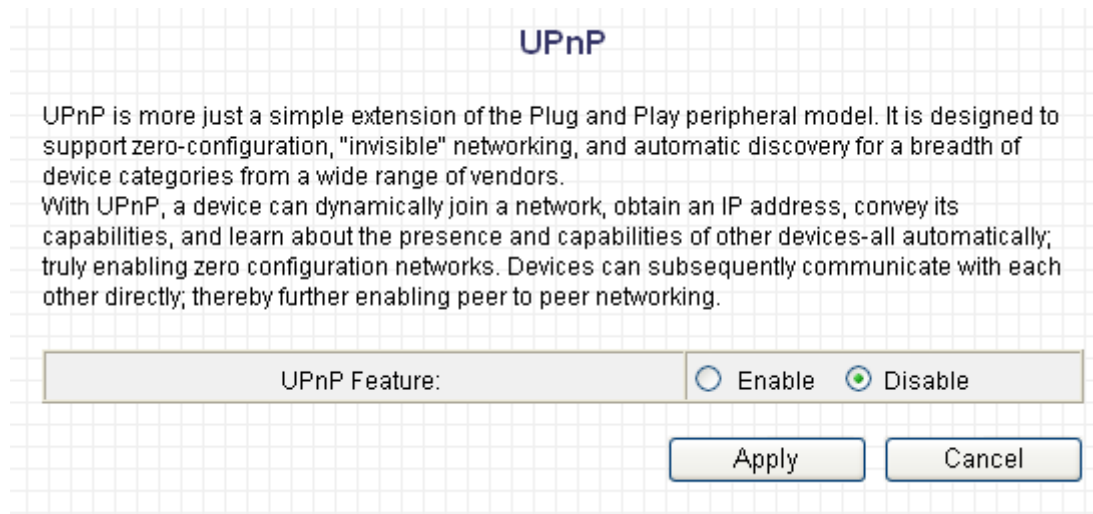
When you finished with the settings in this page, you can click 'Apply' button to save changes you made in this page, or you can click 'Cancel' to discard changes. After you click 'Apply' button, you'll see the following messages:



Please click 'Apply' to save changes you made and restart the broadband router, this requires about 30 seconds and the broadband router will stop responding (this is normal and is not malfunction). You can reconnect to this broadband router and continue on other settings later.

2.7.4 UPnP Settings

With UPnP, all PCs in your Intranet will discover this router automatically. So you do not have to do any configuration for your PC, and they can access the Internet through this router automatically.



UPnP

UPnP is more just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.

With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

UPnP Feature: ☐ Enable ☒ Disable

| Parameters | Default | Description |
|--------------|---------|---|
| UPnP Feature | Disable | You can Enable or Disable UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications which support UPnP smoothly connect to Internet websites and avoid any incompatibility problem due to the NAT port translation. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7.5 ALG Settings

You can select applications that require “Application Layer Gateway” support.

Below are applications that need router's special support to make them work under the NAT. You can select applications that you are using.

| Enable | Name | Comment |
|-------------------------------------|-------------------|--|
| <input checked="" type="checkbox"/> | Amanda | Support for Amanda backup tool protocol. |
| <input checked="" type="checkbox"/> | Egg | Support for eggdrop bot networks. |
| <input checked="" type="checkbox"/> | FTP | Support for FTP. |
| <input checked="" type="checkbox"/> | H323 | Support for H323/netmeeting. |
| <input checked="" type="checkbox"/> | IRC | Allows DCC to work though NAT and connection tracking. |
| <input checked="" type="checkbox"/> | MMS | Support for Microsoft Streaming Media Services protocol. |
| <input checked="" type="checkbox"/> | Quake3 | Support for Quake III Arena connection tracking and nat. |
| <input checked="" type="checkbox"/> | Talk | Allows netfilter to track talk connections. |
| <input checked="" type="checkbox"/> | TFTP | Support for TFTP. |
| <input checked="" type="checkbox"/> | IPsec | Support for IPsec passthrough |
| <input type="checkbox"/> | Starcraft | Support for Starcraft/Battle.net game protocol. |
| <input type="checkbox"/> | MSN | Support for MSN file tranfer. |
| <input checked="" type="checkbox"/> | PPTP Pass Through | Support for PPTP passthrough. |

| Parameters | Default | Description |
|------------|---------|--|
| Enable | | You can enable “Application Layer Gateway” function, and the router will let selected application correctly pass though the NAT gateway. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.7.6 Static Routing

This router provides static routing function when NAT is disabled. With static routing, the router can forward packets according to your routing rules. The IP sharing function will not work any more in static routing mode.

Note: The DMZ function of firewall will not work if static routing is enabled.

NAT ?

NAT (Network Address Translation) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as the Web or FTP.

NAT Module : ☐ Enable ☒ Disable

APPLY

Static Routing

You can enable Static Routing to turn off NAT function of this router and let this router forward packets by your routing policy.

☐ Enable Static Routing

| Destination LAN IP | Subnet Mask | Default Gateway | Hop Count | Interface |
|----------------------|----------------------|----------------------|----------------------|-----------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | LAN ▾ |

Add Reset

Current Static Routing Table

| NO. | Destination LAN IP | Subnet Mask | Default Gateway | Hop Count | Interface | Select |
|-----|--------------------|-------------|-----------------|-----------|-----------|--------|
|-----|--------------------|-------------|-----------------|-----------|-----------|--------|

Delete Delete All Reset

APPLY CANCEL

| Parameters | Description |
|-----------------------|---|
| Enable Static Routing | Static routing function is disabled by default. You have to enable the static routing function, to make your routing rules take effect. |
| Destination LAN IP | The network address of destination LAN. |
| Subnet Mask | The subnet mask of destination LAN. |
| Default | The next stop gateway of the path toward the |

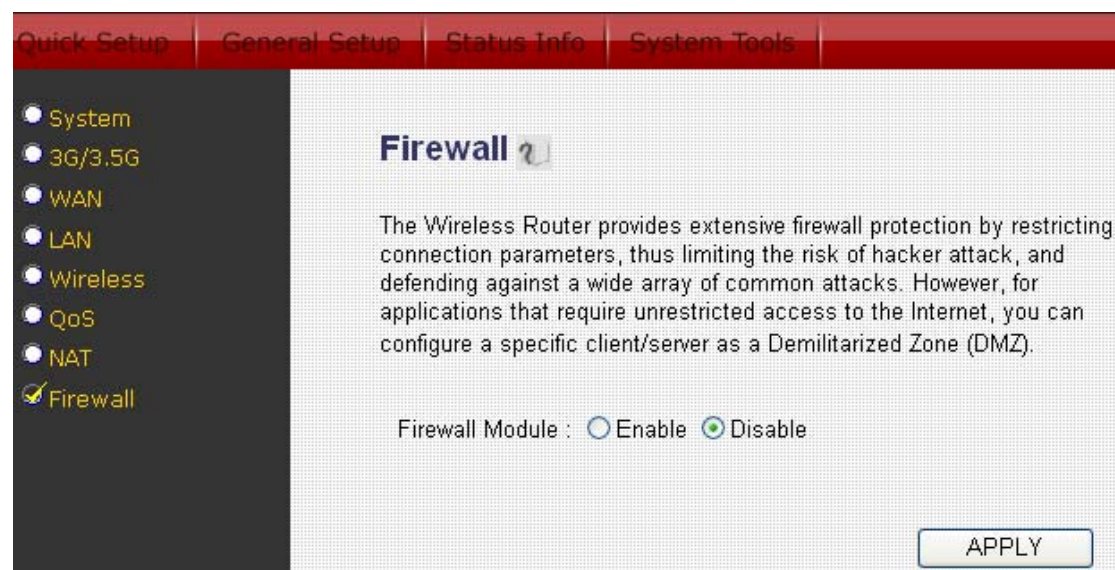
| | |
|---------------|--|
| Gateway | destination LAN. This is the IP of the neighbor router that this router should communicate with on the path to the destination LAN. |
| Hop Count | The number of hops (routers) to pass through to reach the destination LAN. |
| Interface | The interface that go to the next hop (router). |
| Add a Rule | Fill in the "Destination LAN IP", "Subnet Mask", "Default Gateway", "Hop Count" and "Interface" of the rule to be added and click "Add". Then this static routing rule will be added to the "Static Routing Table" listed below. If you found any typo before adding it and want to correct it, just click "Reset" and the fields will be cleared. |
| Remove a Rule | If you want to remove some routing rules from the "Static Routing Table", select the rules you want to remove in the table and click "Delete Selected". If you want remove all rules from the table, just click "Delete All" button. Click "Reset" will clear your current selections. |

Click <**Apply**> at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.8 Firewall

This broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server to be located in Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select **Enable** and click **Apply**



| Parameters | Description |
|------------|---|
| Access | Access control allows you to specify which computer |

| | |
|--------------|---|
| Control | can or cannot access to certain Internet applications |
| URL Blocking | URL Blocking allows you to specify which URLs can not be accessed by users. |
| DoS | The Broadband router's firewall can block common hacker attacks and can log the attack activities. |
| DMZ | The DMZ function allows you to redirect all packets going to your WAN port IP address to a particular IP address in your LAN. |

Click on one of the firewall selections and proceed to the manual's relevant sub-section

2.8.1 Access Control

If you want to restrict users from accessing certain Internet applications /services (e.g. Internet websites, email, FTP etc.), this is the place to set that configuration. Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services in which they can have access to these services. If both of MAC filtering and IP filtering are enabled simultaneously, the MAC filtering table will be checked first and then IP filtering table.

☐ Enable MAC Filtering ☒ Deny ☐ Allow

| Client PC MAC Address | Computer Name | Comment |
|-----------------------|------------------------|---|
| <input type="text"/> | << -----Select----- >> | <input type="text"/> |
| | | <input type="button" value="Add"/> <input type="button" value="Reset"/> |

Current MAC Filtering Table

| NO. | Computer Name | Client PC MAC Address | Comment | Select |
|-----|---------------|-----------------------|---------|--|
| | | | | <input type="button" value="Delete"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> |

☐ Enable IP Filtering ☒ Deny ☐ Allow

| NO. | Client PC Description | Client PC IP Address | Client Service | Protocol | Port Range | Select |
|-----|-----------------------|----------------------|----------------|----------|------------|---|
| | | | | | | <input type="button" value="Add PC"/> <input type="button" value="Delete"/> <input type="button" value="Delete All"/> |
| | | | | | | <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/> |

Here are descriptions of every setup items:

| Item Name | Description |
|-----------------------------|---|
| <i>Enable MAC Filtering</i> | <i>Check this box to enable MAC address based filtering, and please select 'Deny' or 'Allow' to</i> |

| | |
|------------------------------|---|
| | <i>decide the behavior of MAC filtering table. If you select deny, all MAC addresses listed in filtering table will be denied from connecting to the network; if you select allow, only MAC addresses listed in filtering table will be able to connect to the network, and rejecting all other network devices.</i> |
| <i>Client PC MAC address</i> | <i>Please input the MAC address of computer or network device here, dash (-) or colon (:) are not required. (i.e. If the MAC address label of your wireless device indicates 'aa-bb-cc-dd-ee-ff' or 'aa:bb:cc:dd:ee:ff', just input 'aabbccddeeff')</i> |
| <i>Computer Name</i> | <p><i>All computer names found by this broadband router on local network will be listed here. You can select the computer name and click '<<' button to add selected computer's IP address to 'Private IP' field.</i></p> <p><i>Please note that this list may not be able to list all computers on your local network.</i></p> |
| <i>Comment</i> | <i>You can input any text here as the comment of this MAC address, like 'ROOM 2A Computer' or anything. You can input up to 16 alphanumerical characters here. This is optional and you can leave it blank, however, it's recommended to use this field to write a comment for every MAC addresses as a memory aid.</i> |
| <i>Add</i> | <i>Click 'Add' button to add the MAC address and associated comment to the MAC address filtering table.</i> |
| <i>Reset</i> | <i>Remove all inputted values.</i> |

All MAC address entries will be listed in this page:

| MAC Filtering Table | | | | |
|---------------------|---------------|-----------------------|-----------|--------------------------|
| NO. | Computer name | Client PC MAC address | Comment | Select |
| 1 | OFFLINE | aa:bb:cc:dd:ee:ff | Office PC | <input type="checkbox"/> |
| 2 | OFFLINE | 11:22:33:44:55:66 | lab 1 | <input type="checkbox"/> |

To delete one or more entries listed here, please check the box of the mapping entry (under 'Select'), and click 'Delete Selected' button.

If you wish to delete all mapping entries, click 'Delete All' button. To deselect all checked boxes, click 'Reset' button.

If you wish to use IP address-based filtering, please use 'IP Filtering Table' in this page:

☐ Enable IP Filtering Table (up to 20 computers) ☒ Deny ☐ Allow

| NO. | Client PC Description | Client PC IP address | Client Service | Protocol | Port Range | Select |
|-----|-----------------------|----------------------|----------------|----------|------------|--------------------------|
| 1 | POS | 192.168.98.150 | E-mail Sending | | | <input type="checkbox"/> |

Please check 'Enable IP Filtering Table' box first, and select 'Deny' or 'Allow' to decide the behavior of IP filtering table (Deny the access of IP addresses in the list, or allow the access of IP addressees in the list). You have to click 'Add PC' button to add a new IP address to the list:

Access Control Add PC

This page allows users to define service limitation of client PC, including IP address and service type.

| | |
|-------------------------|---|
| Client PC Description : | <input type="text"/> |
| Client PC IP address : | <input type="text"/> . <input type="text"/> |

Here are descriptions of every setup items:

| Item Name | Description |
|------------------------------|---|
| <i>Client PC Description</i> | <i>Please input any text to describe this IP address, up to 16 alphanumerical characters.</i> |
| <i>Client PC IP address</i> | <i>Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address.</i> |

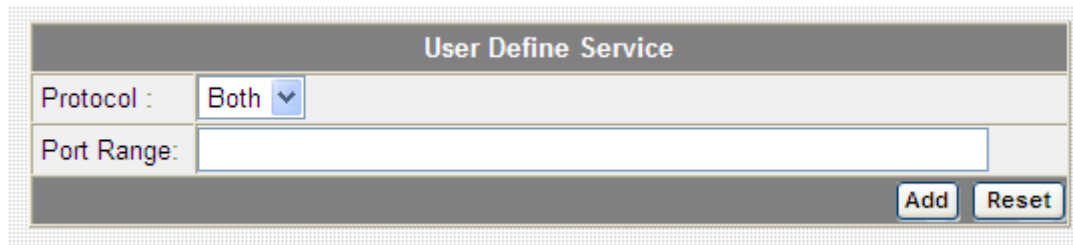
You also have to select the type of Internet services that will be applied to this access control rule from the list:

| Client PC Service : | | |
|---------------------|---|--------------------------|
| Service Name | Detail Description | Select |
| WWW | HTTP, TCP Port 80, 3128, 8000, 8080, 8081 | <input type="checkbox"/> |
| E-mail Sending | SMTP, TCP Port 25 | <input type="checkbox"/> |
| News Forums | NNTP, TCP Port 119 | <input type="checkbox"/> |
| E-mail Receiving | POP3, TCP Port 110 | <input type="checkbox"/> |
| Secure HTTP | HTTPS, TCP Port 443 | <input type="checkbox"/> |
| File Transfer | FTP, TCP Port 21 | <input type="checkbox"/> |
| MSN Messenger | TCP Port 1863 | <input type="checkbox"/> |
| Telnet Service | TCP Port 23 | <input type="checkbox"/> |
| AIM | AOL Instant Messenger, TCP Port 5190 | <input type="checkbox"/> |
| NetMeeting | H.323, TCP Port 389,522,1503,1720,1731 | <input type="checkbox"/> |
| DNS | UDP Port 53 | <input type="checkbox"/> |
| SNMP | UDP Port 161, 162 | <input type="checkbox"/> |
| VPN-PPTP | TCP Port 1723 | <input type="checkbox"/> |
| VPN-L2TP | UDP Port 1701 | <input type="checkbox"/> |
| TCP | All TCP Port | <input type="checkbox"/> |
| UDP | All UDP Port | <input type="checkbox"/> |

You can select multiple services here. If you wish to deny or allow all services of certain IP address(es), please select both 'TCP' and 'UDP'.

If the service you wish to deny or allow is not listed, you can use 'User Define

Service' table to add a new service of your own:

A screenshot of a web form titled "User Define Service". It contains two input fields: "Protocol :" with a dropdown menu showing "Both" and a small downward arrow, and "Port Range:" with a text input field. At the bottom right of the form are two buttons: "Add" and "Reset".

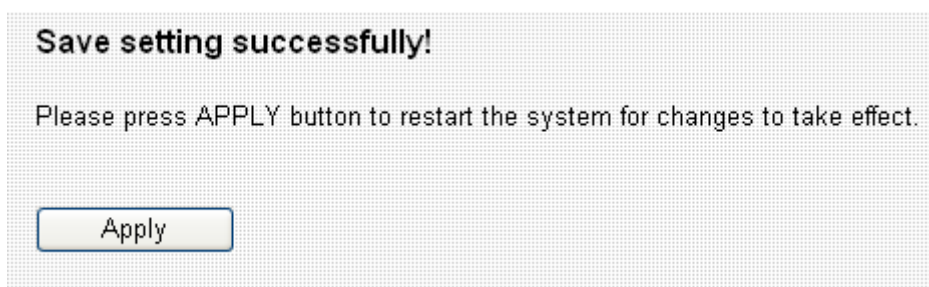
| User Define Service | |
|----------------------|----------------------|
| Protocol : | Both ▼ |
| Port Range: | <input type="text"/> |
| <div>Add Reset</div> | |

Here are descriptions of every setup items:

| Item Name | Description |
|------------|--|
| Protocol | Please select the protocol type of this service: TCP or UDP, or 'Both'. |
| Port Range | <p>Please input the port range if this service. For a single port number, just input the number of service port (like '110').</p> <p>If this service consists multiple continuous ports, you can input '110-120' for port number 110 to 120, or '110,115,120' for port number 110, 115, and 120.</p> |

Click 'Add' to add this IP address restriction rule to the list (and back to previous page), or click 'Reset' to clear all texts in every field.

When you finished with the settings in this page, you can click 'Apply' button to save changes you made in this page, or you can click 'Cancel' to discard changes. After you click 'Apply' button, you'll see the following messages:

A screenshot of a message box with a light gray background. It contains the text "Save setting successfully!" in bold, followed by "Please press APPLY button to restart the system for changes to take effect." At the bottom is a button labeled "Apply".

Save setting successfully!

Please press APPLY button to restart the system for changes to take effect.

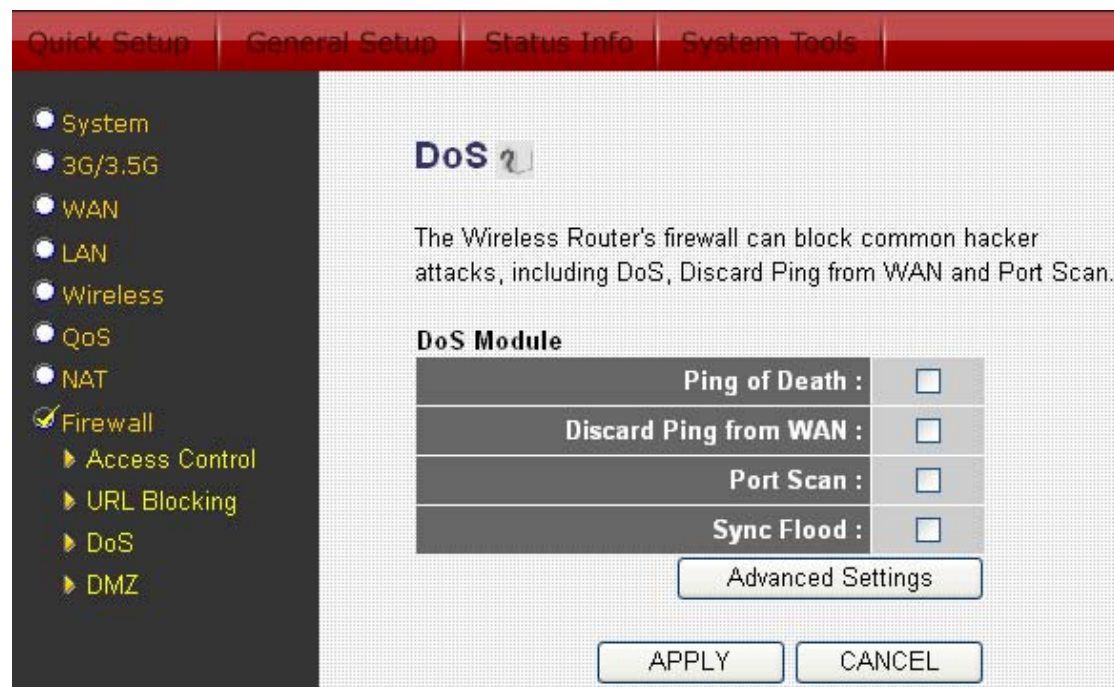
Apply

| | |
|-----------------------|---|
| Add URL Keyword | Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block. If you found any typo before adding it and want to correct it, just click "Reset" and the field will be cleared. |
| Remove URL Keyword | If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset". |

You can now configure other advance sections or start using the router.

2.8.3 DoS (Denial of Service)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.



| Parameters | Description |
|-----------------------|---|
| Ping of Death | Protect from Ping of Death attack |
| Discard Ping From WAN | The router's WAN port will not respond to any Ping requests |
| Port Scan | Protect the router from Port Scan. |
| Sync Flood | Protect the router from Sync Flood attack. |

Click **<Apply>** at the bottom of the screen to save the configurations. You can now configure other advance sections or start using the router.

2.8.4 DMZ

If you have a local client PC that cannot run some specific Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to redirect all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server redirects a particular service/Internet application to a particular LAN client/server, whereas DMZ redirects all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

DMZ

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

☐ Enable DMZ

| Public IP | Client PC IP Address | Computer Name |
|--|----------------------|--|
| <input checked="" type="radio"/> Dynamic IP <div> Session 1 <div></div> </div> | <input type="text"/> | <div> << -----Select----- <div></div> </div> |
| <input type="radio"/> Static IP <div> <input type="text"/> </div> | <input type="text"/> | <div> << -----Select----- <div></div> </div> |

• Current DMZ Table

| NO. | Computer Name | Public IP | Client PC IP Address | Select |
|-----|---------------|-----------|----------------------|--|
| | | | | <input type="button" value="Delete"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/> |

| Parameters | Description |
|----------------------|---|
| Enable DMZ | Enable/disable DMZ Note: If there's confliction between the virtual server and the DMZ setting, the virtual server function will have priority over the DMZ function. |
| Public IP Address | The IP address of the WAN port or any other public IP addresses assigned to you by your ISP. |
| Client PC IP Address | Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address listed above. Note: You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly. |

Chapter 3

Status

The Status section allows you to monitor the current status of your router. You can use the Status page to monitor: the connection status of the Broadband router's WAN/LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.

Quick Setup | **General Setup** | **Status Info** | **System Tools**

✓ **Status**
▶ Internet Connection
▶ Device Status
▶ System Log
▶ Security Log
▶ Active DHCP Client
▶ Statistics

Current Time
3/11/2009 9:37:23

Status

The Wireless Router's status information provides the following information about your Wireless Router: Hardware/Firmware version, Serial Number, and its current operating status.

| System | |
|-------------------------------|-----------------------------|
| Model : | 3G-6200N Wireless 3G Router |
| Up Time : | 0day:0h:0m:33s |
| Hardware Version : | Rev. A |
| Boot Code Version : | 1.0 |
| Runtime Code Version : | 2.03 |

| Parameters | Description |
|------------------------|--|
| Status and Information | Shows the router's system information |
| Internet Connection | View the Broadband router's Internet connection status and other related information |
| Device Status | View the Broadband router's current settings |
| System Log | View the Broadband router's system log |
| Security Log | View any attempts that have been made to gain access to your network. |
| Active DHCP Client | View your LAN client's information that is currently linked to the broadband router |
| Statistics | Shows the statistics |

Select one of the above Status selections and proceed to the manual's relevant sub-section

Status and Information

The Status and Information section allows you to view the router's system information

Quick Setup | **General Setup** | **Status Info** | **System Tools**

Status

- Internet Connection
- Device Status
- System Log
- Security Log
- Active DHCP Client
- Statistics

Current Time
3/11/2009 9:37:23

Status

The Wireless Router's status information provides the following information about your Wireless Router: Hardware/Firmware version, Serial Number, and its current operating status.

| System | |
|-------------------------------|-----------------------------|
| Model : | 3G-6200N Wireless 3G Router |
| Up Time : | 0day:0h:0m:33s |
| Hardware Version : | Rev. A |
| Boot Code Version : | 1.0 |
| Runtime Code Version : | 2.03 |

| Parameters | Description |
|-------------|--|
| Information | You can see the router's system information, such as the router's LAN MAC address, WAN MAC address, hardware version, serial number, boot code version, runtime code version |

3.1 Internet Connection

View the Broadband router's current Internet connection status and other related information

View the current internet connection status and related information.


| | |
|-----------------------------|-----------------------|
| Attain IP Protocol : | Dynamic IP disconnect |
| IP Address : | |
| Subnet Mask : | |
| Default Gateway : | 192.168.9.254 |
| MAC Address : | 00:1F:1F:1F:74:51 |
| Primary DNS : | 192.168.1.2 |
| Secondary DNS : | 192.168.1.12 |

| | |
|----------------------|--------------|
| WWAN Status: | Disconnected |
| IP Address: | N/A |
| Subnet Mask: | N/A |
| Gateway: | N/A |
| Manufacturer: | N/A |
| Product: | N/A |

| Parameters | Description |
|---------------------|---|
| Internet Connection | This page displays the router's WAN port and 3G/3.5G Internet (WWAN) connection information, including: WAN IP address, subnet mask, and ISP gateway as well as the primary DNS and secondary DNS being used. |

3.2 Device Status

View the broadband router's current configuration settings. The device status displays the configuration settings you've configured in the Quick Setup Wizard/General Setup section.

Device Status 

View the current setting status of this device.

Wireless Configuration

| | |
|-------------------------|--------------|
| Mode : | Access Point |
| ESSID : | default |
| Channel Number : | 11 |
| Security : | Disable |

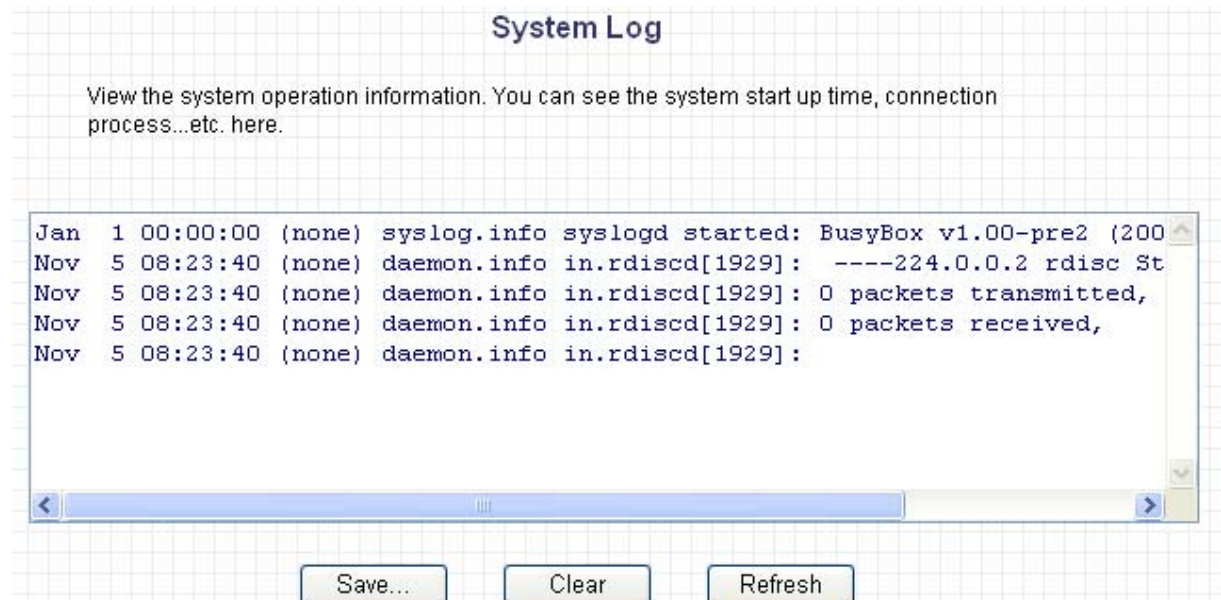
LAN Configuration

| | |
|----------------------|-------------------|
| IP Address : | 192.168.2.1 |
| Subnet Mask : | 255.255.255.0 |
| DHCP Server : | Enable |
| MAC Address : | 00:1f:1f:1f:74:50 |

| Parameters | Description |
|---------------|--|
| Device Status | This page shows the broadband router's current device settings, including: broadband router LAN port's current LAN IP address and subnet mask. It also shows whether the DHCP server function is enabled / disabled. |

3.3 System Log

View the operation log of the system.



| Parameters | Description |
|------------|--|
| System Log | <p>This page shows the system log of the broadband router. It displays any event occurred after system start up.</p> <p>At the bottom of the page, the system log can be saved <Save> as a local file, you can clear the log by click <Clear> button, too. You can also click <Refresh> button to get the most updated information. When the system is powered down, the system log will disappear if it's not saved as a local file.</p> |

3.4 Security Log

View any attempts that have been made to gain access to your network.



| Parameters | Description |
|--------------|---|
| Security Log | <p>This page shows the current security log of the Broadband router. It displays all attempts tried to access your network.</p> <p>At the bottom of the page, the security log can be saved <Save> as a local file, you can clear the log by clicking <Clear>, too. You can also click <Refresh> button to get the most updated information. When the system is powered down, the security log will disappear if it's not saved as a local file.</p> |

3.5 Active DHCP Client

This page lists all DHCP clients.

Active DHCP Client

This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.


| IP Address | MAC Address | Time Expired (Second) |
|---------------|-------------------|-----------------------|
| 192.168.2.100 | 00:00:00:00:00:00 | 3547 |
| 192.168.2.101 | 00:13:02:5f:ed:e9 | forever |

Refresh

| Parameters | Description |
|--------------------|---|
| Active DHCP Client | This page shows all DHCP clients currently connected to your network. The “Active DHCP Client Table” displays the IP address and the MAC address and expiry time of each LAN Client. Use the Refresh button to get the most updated information. |

3.6 Statistics

View the statistics of packets sent and received on WAN, LAN and Wireless LAN interface.

Statistics 

This page shows the packet counters for transmission and reception regarding to networks.

| | | |
|--------------|------------------|------|
| Wireless LAN | Packets Sent | 107 |
| | Packets Received | 5706 |
| Ethernet LAN | Packets Sent | 302 |
| | Packets Received | 195 |
| Ethernet WAN | Packets Sent | 124 |
| | Packets Received | 514 |

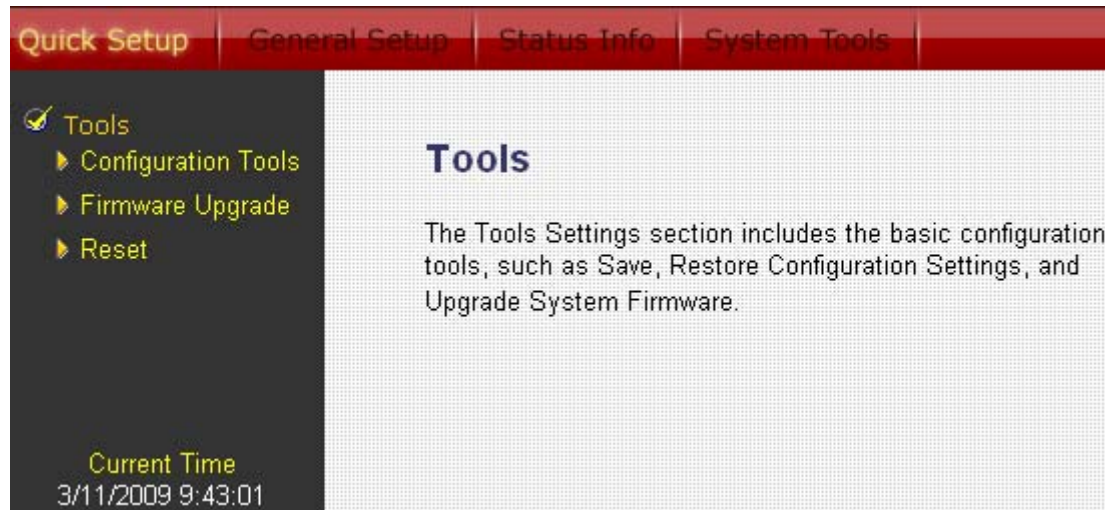
Refresh

| Parameters | Description |
|------------|---|
| Statistics | Shows the statistics of packets sent and received on WAN, LAN and Wireless LAN interface. |

Chapter 4

Tool

This page includes basic configuration tools of this broadband router, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.



| Parameters | Description |
|---------------------|---|
| Configuration Tools | You can save the router's current configuration, restore the configuration from previously saved configuration files, and restore the router's factory default settings |
| Firmware Upgrade | This page allows you to upgrade the router's firmware |
| Reset | When you encounter any problem using this broadband router, you can reset the router by this function |

Select one of the above **Tools Settings** selections and proceed to the relevant sub-section

4.1 Configuration Tools

The Configuration Tools screen allows you to save (**Backup**) the router's current settings. Saving the configuration settings provides an added protection and convenience when there're some problems with the router, and you have to reset to factory default to solve the problem. When you save the configuration setting (Backup), you can reload the saved configuration to the router through the **Restore** selection. If extreme problems occur you can use the **Restore to Factory Defaults**

selection, this will set all configurations to its original default settings (e.g. when you purchased the router).

Configuration Tools ?

Use the "Backup" tool to save the Wireless Router's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Wireless Router. Alternatively, you can use the "Restore to Factory Default" tool to force the Wireless Router to perform System Reset and restore the original factory settings.

| | |
|-------------------------------------|--|
| Backup Settings : | <input type="button" value="Save"/> |
| Restore Settings : | <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/> |
| Restore to Factory Default : | <input type="button" value="Reset"/> |

| Parameters | Description |
|---------------------|---|
| Configuration Tools | Use the " Backup " tool to save the broadband router's current configuration to a file named "config.bin" on your PC. You can then use the " Restore " tool to restore the saved configuration to the broadband router. Alternatively, you can use the " Restore to Factory Defaults " tool to force the broadband router to perform a power reset and restore to original factory settings. |

4.2 Firmware Upgrade

This page allows you to upgrade the router's firmware

| | |
|---|---|
| Quick Setup General Setup Status Info System Tools | <h3>Firmware Upgrade ?</h3> <p>This tool allows you to upgrade the Wireless Router's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.</p> <p>The system will automatically reboot the router after you finished the firmware upgrade process. If you don't complete the firmware upgrade process in the "next" step, you have to reboot the router.</p> <p style="text-align: right;"><input type="button" value="NEXT"/></p> |
|---|---|

Tools

- ▶ Configuration Tools
- ▶ Firmware Upgrade
- ▶ Reset

Current Time
3/11/2009 9:46:13

Firmware Upgrade ?

This tool allows you to upgrade the Wireless Router's system firmware. Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

| Parameters | Description |
|------------------|---|
| Firmware Upgrade | This tool allows you to upgrade the broadband router's system firmware. To upgrade the firmware of your broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also click the browse button to locate the firmware file on your PC. |

After you selected the new firmware file, click **<Apply>** at the bottom of the screen to start the upgrade process. (You may have to wait few minutes for the upgrade to complete). Once the upgrade is complete you can start using the router.

Warning: When upgrading firmware, be sure not to switch the computer off, or restart your computer.

4.3 Reset

You can reset the router's system when there's something wrong with the router. The reset function will reboot your router.

Quick Setup | **General Setup** | Status Info | System Tools

Tools

- Configuration Tools
- Firmware Upgrade
- Reset

Current Time
3/11/2009 9:48:15

Reset ?

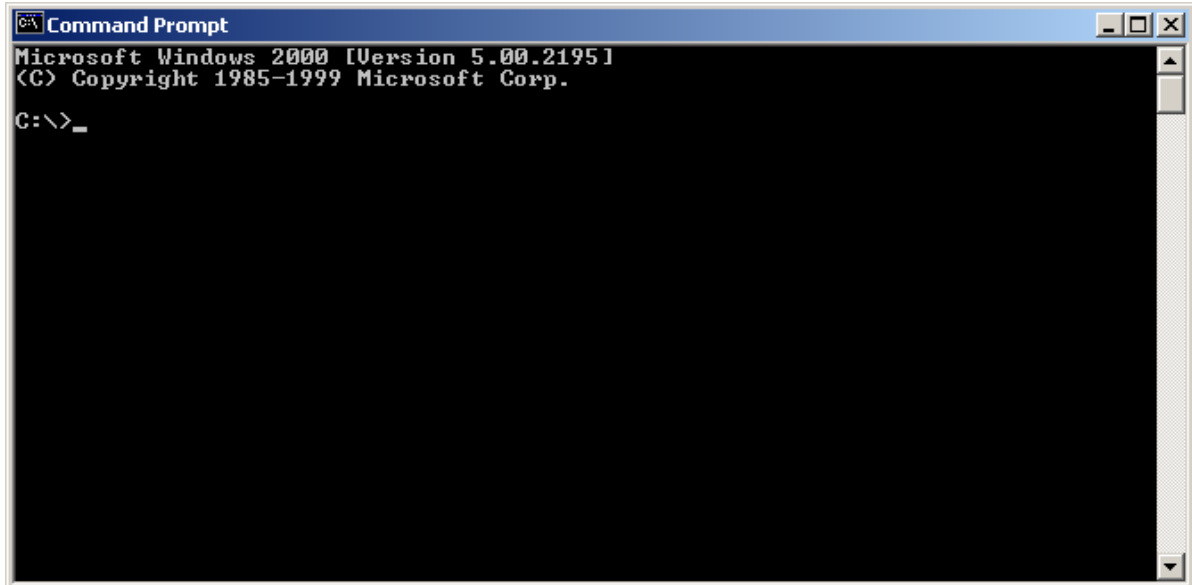
In the event that the system stops responding correctly or stops functioning, you can perform a Reboot. Your settings will not be changed. To perform the reboot, click on the APPLY button below. You will be asked to confirm your decision. The Reboot will be complete when the LED Power light stops blinking.

| Parameters | Description |
|------------|--|
| Reset | In the event that the system stops responding or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the <APPLY> button. You will be asked to confirm your decision. The reset will be complete when the power LED stops blinking. Once the reset process is complete you may start using the router. |

Appendix A

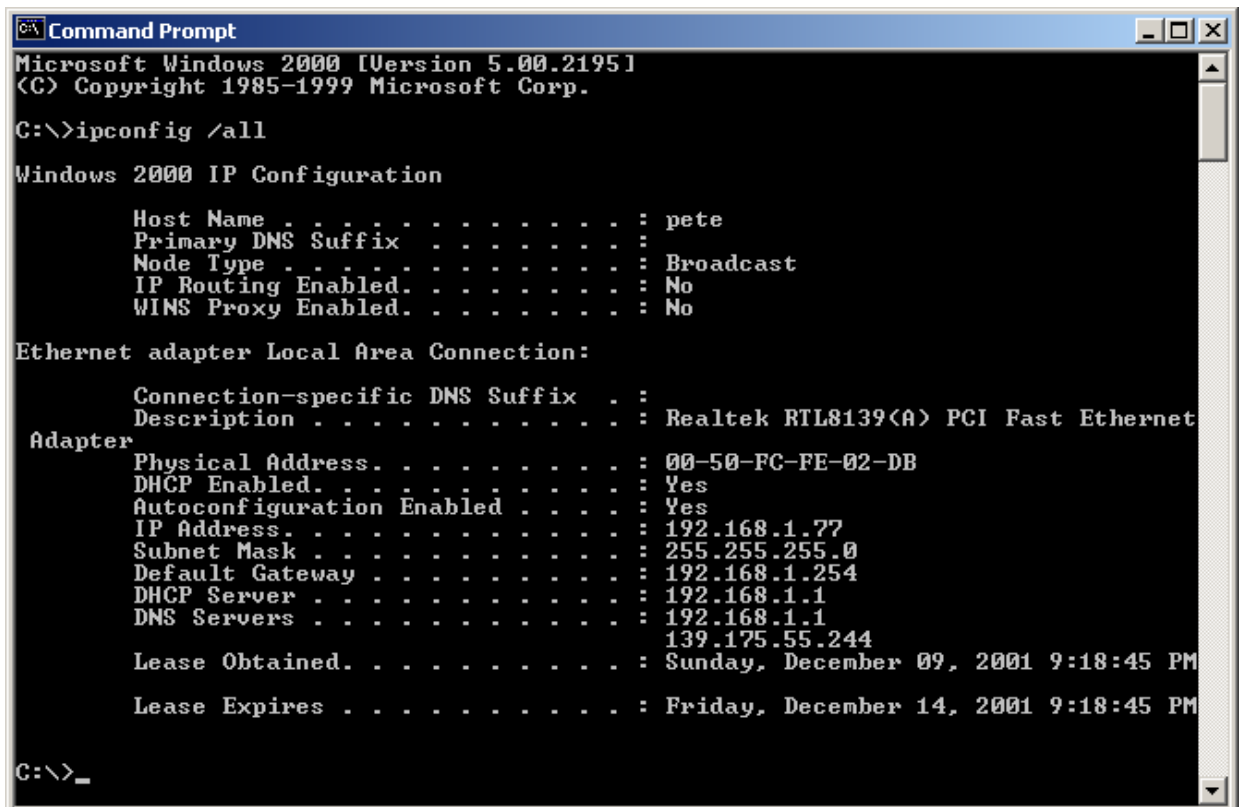
How to find your PC's IP and MAC address manually

1) In Windows open the Command Prompt program



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>_
```

2) Type `Ipconfig /all` and <enter>



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>ipconfig /all

Windows 2000 IP Configuration

    Host Name . . . . . : pete
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
    Adapter
    Physical Address. . . . . : 00-50-FC-FE-02-DB
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.77
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
                           139.175.55.244
    Lease Obtained. . . . . : Sunday, December 09, 2001 9:18:45 PM
    Lease Expires . . . . . : Friday, December 14, 2001 9:18:45 PM

C:\>_
```

- Your PC's IP address is the one titled as **IP address** (192.168.1.77 in this example)
- The router's IP address is the one titled as **Default Gateway** (192.168.1.254 in this example)
- Your PC's MAC Address is the one titled as **Physical Address** (00-50-FC-FE-02-DB in this example)

Glossary

Default Gateway (Router): Every non-router IP device needs a default gateway. When the device sends out an IP packet, if the destination is not in the same network, the device will send the packet to default gateway, which will then forward it to the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically assigns an IP address for every computer in your network.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as `www.Broadbandrouter.com`) and one or more IP addresses (such as `192.34.45.8`). A DNS server will maintain a database of domain names and respective IP addresses, so when a domain name is requested (like typing “Broadbandrouter.com” in your Internet browser), the user will get the corresponding IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A kind of standard of computer networks. Ethernet networks are connected by special cables and hubs, and transfers data at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle timeout is designed so that after no traffic has been transferred to the Internet for a pre-configured amount of time, the connection will be disconnected automatically.

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists four sets of numbers separated by periods, which identifies a single, unique Internet computer host in an IP network. Example: `192.168.2.1`. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by “.”: `aaa.aaa.aaa.aaa`, where each “aaa” can be anything from 000 to 255, or as four cascaded binary numbers separated by “.”: `bbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb`, where each “b” can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1’s followed by consecutive trailing 0’s, such as `11111111.11111111.11111111.00000000`. Therefore sometimes a

network mask can also be described simply as “x” number of leading 1’s. When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1’s in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000 It means the device’s network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: (see ISP listed below for explanations). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered as a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It comprises two parts: 3 bytes of data that corresponds to the Manufacturer ID (which is unique for each manufacturer), plus 3 bytes that are often used as the product’s serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband router’s NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network Clients (LAN PC) uses port numbers to identify one network application/protocol from another. Below is a list of common applications and protocol/port numbers:

| Application | Protocol | Port Number |
|-------------|----------|-------------|
| Telnet | TCP | 23 |

| | | |
|-------------|-----|------|
| FTP | TCP | 21 |
| SMTP | TCP | 25 |
| POP3 | TCP | 110 |
| H.323 | TCP | 1720 |
| SNMP | UCP | 161 |
| SNMP Trap | UDP | 162 |
| HTTP | TCP | 80 |
| PPTP | TCP | 1723 |
| PC Anywhere | TCP | 5631 |
| PC Anywhere | UDP | 5632 |

PPPoE: Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

Protocol: A protocol is a set of rules for interaction agreed between multiple parties so that when they communication with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Stands for Wide Area Network. A network that connects computers located in geographically separated areas (e.g. different

buildings, cities, countries). The Internet is a wide area network, too.

Web-based management Graphical User Interface (GUI): Many devices support graphical user interface that is based on the web browser. This means the user can use their familiar web browser (ex. Netscape or Microsoft Internet Explorer) to control/configure or monitor the device being managed.

Federal Communication Commission Interference Statement

FCC Part 68

This equipment complies with Part 68 of the FCC Rules. On the bottom of this equipment is a label that contains the FCC Registration Number and Ringer Equivalence Number (REN) for this equipment. You must provide this information to the telephone company upon request.

The REN is useful to determine the quantity of devices you may connect to the telephone line and still have all of those devices ring when your number is called.

In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If the modem causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance.

But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment.

If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this modem, please contact your dealer for repair/warranty information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected or you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Installation

This device is equipped with a USOC RJ11C connector.

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio

frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission Radiation Exposure Statement

This equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

The equipment version marketed in US is restricted to usage of the channels 1-11 only.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC

OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Bulgaria, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Romania, Slovakia, Slovenia, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CE Mark Warning

This is a class B product. In a domestic environment, this product may cause radio interface, in which case the user may be required to make adequate measures.

A CE declaration of conformity is available on www.edimax.com





EDIMAX Technology Co., Ltd.

www.edimax.com